January 1991 ISSN 0956-9979

VIRUS BULLETIN

THE AUTHORITATIVE INTERNATIONAL PUBLICATION
ON COMPUTER VIRUS PREVENTION,
RECOGNITION AND REMOVAL

CONTENTS

EDITORIAL

A Matter of Trust

In early December 1990 the *University of Hamburg* hosted an expert meeting on computer viruses and malicious software. An eminent group of virus researchers attended at the invitation of Professor Klaus Brunnstein, head of the university's computing faculty which is the home of the *Virus Test Centre* - a dedicated German computer virus research laboratory. The purpose of the expert meeting was to establish an effective European malicious software research, monitoring and warning service and to provide guidelines for the security and circulation of malicious code. In addition to the research community (which included a high proportion of anti-virus software developers), representatives from academia, business, industry and the police attended.

The meeting and subsequent conference, which included presentations by Fridrik Skulason and Dr. Alan Solomon, proved invaluable. Many key researchers met face-to-face for the first time and were able to discuss pertinent technical and ethical matters. Cooperation between researchers will certainly increase as a result of the Hamburg meeting - e-mail addresses and telephone numbers were exchanged as were samples of virus code and various disassembly and analysis tools including a range of scanners and static-analysis software currently in use in the Soviet Union.

The most alarming trend reported at the conference, and reflected in the *VB Table of Known IBM PC Viruses*, has been the massive proliferation in the number of computer viruses emanating from Eastern Europe and the USSR. Presumably this is the work of a disaffected programming community frustrated by the lack of incentive to develop constructive software. Conference delegates were told that available statistics indicated that the number of separately identifiable computer virus strains will reach 700 by the end of this year and will exceed 1,000 by mid-1992. In line with developments in Bulgaria, it is probable that the majority of malicious software programmed in the former Communist Bloc will be released directly into the wild and that it will become increasingly sophisticated.

The gravity of the situation, compounded this month by the discovery of numerous virus samples in the United States, makes the principal objectives of the Hamburg conference all the more necessary. Indeed, without a concerted and combined effort, it would appear that the conventional response to virus detection will soon become a lost cause. A number of factors militate against cooperation, particularly between commercial organisations (which sell anti-virus software), researchers (many of whom develop shareware) and academics (where research often does not extend to software development).

There are two principal obstacles to harmonised research efforts and software development. The first is ethical - is it justifiable to exploit the computer virus situation for profit as do the commercial software organisations? A body of opinion which opposes commercial involvement in computer virus countermeasures is growing in influence. It argues that remedial software should be provided at the lowest cost to the end-user who should not be penalised for the irresponsible activities of the virus writers. Countering this lobby are those who believe that developing and sustaining effective, professional anti-virus software and providing attendant support and updates is a full-time occupation which necessitates commercial practices.

The second stumbling block is the erroneous belief on the part of some software developers that computer virus code is 'property', to be hoarded and secured from the prying eyes of the competition. The attitude that the "fastest with the mostest" will win the commercial war is strewn with dangers.

A seemingly insoluble problem thus surrounds the secure, trusted circulation of virus code. Each interested party assumes the right to receive virus code but commercial competition and distrust between the various software developers often hinders this process. This problem would be overcome by an independent agency which could vet applicants to receive malicious software. Questions arise. From where would this agency gain its authority? How could it be sponsored? To whom would it be answerable?

If no solutions are forthcoming, the allied (?) combatantsin the 'virus war' will just have to struggle on in an ad hoc, disorganised fashion relying on instinctive trust and distrust.

Helping With Enquiries

The United Kingdom's *Computer Misuse Act*, 29th August, 1990 renders the insertion of viral code into computer systems a criminal offence punishable by a maximum prison sentence of five years.

The *Computer Crime Unit* which is attached to the *City and Metropolitan Police* has established a log of all computer virus outbreaks in the United Kingdom. The unit, currently comprising four detectives, is keen that individuals and organisations should report computer virus infections. Information will yield valuable clues as to the functioning and spread of each virus and may provide the basis for extradition and prosecution in the event that a virus writer is apprehended. In this regard they have asked anyone in the UK experiencing a computer virus infection to contact:

Noel Bonczonzek
Computer Crime Unit
2 Richbell, London WC1X 8SD

Tel 071 725 2409

STOP-PRESS

Mark Hamilton

US Judge Rules In Favour Of Extradition

On 20th December 1990, US District Judge Ann Aldrich ruled that Dr Joseph Popp, a zoologist living in Cleveland, Ohio, should be extradited to the United Kingdom to stand trial for his part in what has become known as the "AIDS Disk incident'' (*VB, January 1990*). In her ruling, the Judge has referred the case to the US *State Department* for its final decision and it must certify that Popp is extraditable under the *Anglo-American Extradition Treaty* of 1972.

According to Cleveland's District Attorney, Matt Cain, Popp must apply for a writ of Habeas Corpus and lodge an appeal by January 20th if he is to avoid extradition at this time. No such writ has been applied for, as yet, according to sources at the *District Court* and the *District Attorney*. Popp has three courses of action open to him. First, he could elect not to appeal and take his chances in the English Courts -informed sources believe this is the most likely outcome. Alternatively, he could appeal to the *District Court* but in this case the appeal would be before Judge Aldrich's Court. Alternatively, he could take the case to the US *Court of Appeal* at the *Supreme Court*, but our sources rule out this possibility on the grounds of its very high cost and uncertain outcome.

Judge Aldrich's decision comes nearly four months after the extradition hearing in August 1990. The judgment ends nine months of uncertainty following Popp's arrest by the *FBI* last March. The AIDS Disk incident was the largest computer crime investigation yet undertaken - involving police forces from 20 countries as well as regional forces in the UK coordinated by the *Computer Crime Unit* based in Holborn, London.

The Charge

That on 11th December 1989, within the jurisdiction of the central Criminal Court, you with a view to gain for another, vis PC Cyborg Corporation of Panama, with menaces made unwarranted demand, vis a payment of one hundred and eighty nine U.S. dollars or three hundred and seventy eight U.S. dollars from the victim.

Popp is charged with blackmail; his arrest on 1st February 1990 preceded the passage of the United Kingdom *Computer Misuse Act* of August 1990, which specifically renders the unauthorised modification of computer data a criminal offence (*English Law Commission* report 186 (para 3.65 (2)). If convicted, Popp faces a maximum sentence of fourteen years' imprisonment for each count of blackmail.

TECHNICAL NOTE

Delayed Replication

Early parasitic viruses replicated in one of two ways. Some, such as Vienna, looked for files to infect when an infected program was executed while others, such as Jerusalem, waited resident in memory to infect programs as they were run.

A number of virus samples obtained for recent analysis have failed to replicate under test conditions. We have now encountered several computer viruses which will not infect other programs until some specific condition is met. To date three types of conditions have been identified:

_ Conditions which provide delays

_ Operating system requirements

_ Hardware requirements

A virus may wait before it starts infecting programs for a fixed time or until other conditions are met - e.g. a certain number of keypresses or disk accesses occur. It may also elect not to infect every program executed; the Icelandic virus which infects one in ten programs executed is an example. The purpose of this delay is to reduce the likelihood of detection although it also retards the spread of infection. The process also impedes analysis as the virus must be disassembled before the necessary number of samples can be created for structural analysis.

Other viruses check the operating system and return control to the original program if the version falls below a specific release number. Some of the Russian viruses will not infect unless the processor is running DOS 3.3 or higher. The reason is simple - the viruses exploit undocumented DOS features which are only found in DOS 3.3 and later versions.

Finally, a virus may not activate unless the machine has a specific hardware configuration - typically, a hard disk. This impedes virus disassembly which is usually undertaken on floppy-drive-only processors. A virus which will only infect in the presence of a loaded and functioning hard disk will, by necessity, take longer to analyse. Some computer viruses which contain code to damage the contents of the hard disk cease replicating should no fixed drive (target) be located.

There are, of course, viruses which crash when used on certain types of hardware - the Italian virus, for example, will not work on a 80286 or 80386 processor. This is probably a 'bug' in the code rather than an intentional effect.

In the *Table of Known IBM PC Viruses* (pp. 5 - 21), hexadecimal patterns for non-replicating specimens have been included on the assumption that the sample **will** replicate if certain (as yet, undetermined) conditions are met.

FROM THE FIELD

A Warning to AUTOCAD Users

The Plastique virus, of which there are currently six variants, is believed to originate from Taiwan. It has been found at sites in Europe and the United Kingdom, probably imported on bootleg software from the Far East where it has become a widespread and genuine menace. The name 'Plastique' is derived from a text string contained in a 4096 byte variant. This name, which refers to plastic explosive, is highly appropriate - the virus will trigger ('explode') causing devastating destruction to any fixed disk(s).

Of critical importance: the destructive routine triggers when the ubiquitous AUTOCAD~ program (ACAD.EXE) is executed. The Plastique virus is also known as AntiCAD.

Technical Analysis

The version analysed here is the 2900 byte variant which has been found at sites in the United Kingdom and Europe.The other variants are awaiting disassembly.

The virus is parasitic on COM and EXE files but does not infect COMMAND.COM. The infection method is slightly unusual in that COM files have the virus code *prepended* to the file, while EXE files have it *appended*. In either case, the infective length is 2900 bytes and no stealth capabilities exist to mask this increase in file length. After infection, file attributes and date/time settings are restored to their original values. The virus code is partially encrypted but allows the extraction of a recognition pattern.

This virus becomes resident in high memory by using the DOS Terminate and Stay Resident (TSR) function 31H. During installation a timing routine determines the processing speed and this is used for sound-effects later. As it becomes resident, INT 21H is intercepted by a special handler which will cause file infection on function requests 4B00H and 3D00H, these correspond to Load and Execute, and Open file for Read Only. The DOS Critical Error handler (INT 24H) is bypassed during the infection cycle to avoid error messages.

On a random basis, virus installation after 20th Sept 1990 may cause other handlers to be installed which produce certain sound-effects and may execute the trigger routine. One of two INT 08H - Timer Interrupt handlers are installed (chances are even of either handler being installed).

_ Handler 1 increments a timer counter and slows processing to a limit decided during installation timing.

_ Handler 2 also increments the timer counter and makes an explosion noise about every 4.5 minutes.

An INT 09 - Keyboard Interrupt handler is installed which will intercept a Ctrl-Alt-Del key sequence and then act accordng to which INT 08 handler is installed. If Handler 1 is present then the trigger routine is activated. If Handler 2 is present then non-volatile RAM is overwritten with 0FFH bytes. The INT 09 handler also counts keypresses and after 4000 keypresses, an error will be forced on the next disk write request to INT 13H

An INT 13H - Disk Access handler is installed which intercepts write requests and forces an error according to the condition of a flag. The error consists of putting -1 into DX (Head and Drive) and completing the call. The routine then returns without setting the relevant flags so that the caller is not aware that his data has not been written.

Trigger Routine

The Trigger routine occurs immediately on execution of ACAD.EXE, otherwise during a Ctrl-Alt-Del sequence from within INT 09H handler if INT 08H Handler 1 is installed and the timer counter has reached a predetermined limit.

The actual routine checks if there is a floppy disk in drive A:, if so it overwrites head 0 of all tracks with the contents of memory from address 0000:0000. Processing continues similarly for floppy in drive B:, zapping it if possible.

Then the "explosion" routine is set to occur as both the first and second fixed disk drives are overwritten on all heads and tracks. Finally a loop overwrites the contents of CMOS by direct port access.

Self Recognition

The virus recognises itself in memory by issuing an INT 21H call with 4B40H in the AX register. If the virus is resident, the call returns with 5678H in AX. Recognition on disk is by examining the word at offset 12H in the target file. If this word is 1989H then the file is assumed to be infected.

Detection

The recognition string for the Plastique (2900) virus is as follows:

```
B840 4BCD 213D 7856 7512 B841 4BBF 0001 ;   Offset
82CH
```

A variant, not detected by this pattern, has been identified in the United States. The following supplementary pattern will detect this variant listed as Plastique (2):

```
CO8E D8A1 1304 B106 D3E0 8ED8 33F6 8B44
```

See the entry in the *VB Table of Known IBM PC Viruses* for further information.

COUNTERMEASURES

Disinfection Software

During recent testing of the effects of data corruption experienced after an infection of the 4K virus, it was noted that commercially available disinfection routines were not as effective as they claimed to be (*VB*, November 1990, pp. 5-6). These routines were put aside until the 4K problem was completely resolved but they have since been examined in greater detail and the results that were obtained have led to the following discussion of disinfection techniques and the associated pitfalls which may be encountered.

File Restoration

The actual process of disinfection must first be defined as returning a file (or disk sector) back to **exactly** the condition it was in prior to being infected by virus code. This will include the restoration of content, length, attributes, date/time settings and possibly even the cluster location on the disk (for copy-protected software). It may well be that restoration of all of the above items is unnecessary in most instances, but there are certainly occasions when they are all needed for the appropriate software to function correctly.

While there is an obvious division between parasitic and boot sector virus disinfection, there is the less obvious categorisation between a generic and specific approach. The virus-generic versus virus-specific argument has caused much heated discussion in virus research circles for some time now; it is not the intention to enter into this debate in this article except where it affects disinfection capabilities.

Boot Sectors

Let us first consider boot sector viruses - while these are the most awkward for ordinary users to recover from, they are actually the easiest as far as disinfection software is concerned.

Virus-specific disinfection software will contain accurate details of the virus concerned and by using this information will be able to locate the original (uninfected) copy of whichever boot sector has been affected. It is then a simple matter of replacing the infected copy with the clean one.

Virus-generic software on the other hand, can work in one of two ways - if a clean copy of the various system sectors has been taken and stored prior to any infection, it is a simple matter to repair any infection. Alternatively, it is often possible to reconstruct the relevant sector by specific system reference. Either way, the sector(s) can be repaired without reference to the capabilities of the particular virus in question as long as the machine is running on a trusted (ie: clean) operating system.

Most boot sector viruses cause no permanent damage during their infection routine, but there are some (notably the New Zealand virus) which can cause damage on certain machine types. In these cases, simple disinfection may not be possible and the user may have to resort to the ultimate option of reformatting the disk.

Reformatting

This is probably an ideal place to clear some of the misunderstandings about disk reformatting as a disinfection exercise. Under most MS-DOS operating systems, the very first sector on the disk (identified as sector 1, track zero, head zero) contains the **Master Boot Sector**. This is always loaded into memory when the machine is booted and it contains the **Partition Record**, a 64 byte table which lists exactly how distinct areas of the disk have been allocated.

Now consider a disk which has been partitioned into two separate drives (usually C: and D:). The Partition Record contains the starting and finishing address of each partition (in absolute terms of track/head/sector numbers) as well as the type, status and other details about it. Users will be aware that if they have a hard disk partitioned in this way, it is easily possible to format either drive C: (first partition) or drive D: (second partition) without damaging data stored on the other partition. Thus it can be appreciated that the ordinary DOS FORMAT command does not affect the entire disk. Even if the physical drive contains only one partition, FORMAT will not touch the Master Boot Sector. **So, if a virus has modified the Master Boot Sector it cannot be removed by an ordinary format**. A special, highly machine-specific, low-level formatting routine is required, followed by reconfiguration and re-partitioning with the DOS FDISK program.

Just as the first sector of the physical disk contains the Master Boot Sector, so the first sector of each partition will contain a **DOS Boot Sector** (logical sector 0 in each DOS partition). If there is more than one partition, one of them will be marked within the Partition Record as "active" and the DOS Boot Sector of this partition will also be loaded into memory when the machine is booted. **Obviously, viruses which only infect the DOS Boot Sector can be destroyed by the normal DOS FORMAT command.**

Parasitic Virus Disinfection

Files infected by parasitic viruses present a different range of problems for disinfection software.

The most reliable and secure method of disinfection is still to delete the infected file using the DOS DEL commandor, preferably, a positive overwriting utility (see 'Secure Erasure', *VB*, November 1990, p. 9)**. Restoration follows using clean write-protected copies of verified and write-protected master disks.**

However, this may be inconvenient - the master disk may not readily be available - it may itself have become damaged or corrupted - there may not even be a master disk! Whatever the reason, the user may be attracted by the possibility of quick and easy virus "removal" facilities being offered as part of an anti-virus package. This is where virus-specific software can be a real boon (always assuming that the offending virusis "known" to the software).

Most parasitic viruses infect files by appending the virus code to the end of the existing file and then modifying the original file contents so that processing is routed through the virus code first. In these cases, the virus will usually repair the original file contents so that the host program will continue to function correctly. For these viruses, disinfection is simply a matter of detecting the section of virus code which does the repair and using the details that it contains to effect a permanent repair before actually removing the virus code from the end of the file.

The problems arise from two directions - if the virus is of the 'stealth' type, it may fool the operating system to such an extent that any self-checking mechanisms within the host program will "see" a clean file exactly as intended. However, once the stealth characteristics are removed from the system, the actual repair of the file may not be accurate enough to restore the file to full health.

This is actually the case with at least three software "cure" packages which attempt disinfection of the 4K (Frodo) virus. In this case, the virus code is appended to the host file and aligned on a paragraph boundary. The repair of the header section of the file may be perfectly alright but removing the virus code can leave the small offset used for paragraph alignment. On ordinary program files this causes no problems but on protected files with self-checking routines the extra bytes cause the protection mechanisms to trigger and prevent program operation. On data files, the presence of any extra bytes will of course produce totally unpredictable results.

On a machine with large numbers of infected files, there is no doubt that a virus-specific disinfection capability could be an enormous time-saver but if the implementation is anything other than 100 percent effective it is best avoided.

Generic Implementations

Few implementations of virus-generic recovery software have yet been seen and this may be because the processes involved in preparing this method are somewhat more time-consuming. Nevertheless, given accurate and well written code, this method promises much.

The theory is as follows: assume a program exists which will automatically take an exact copy of all specified files (just like a backup) and store them somewhere. This program is also capable of replacing the originals with the copies on command.

Once the copies have been taken, any parasitic virus infection can be cured by simply restoring the copies and rewriting them over the originals. The difficulty is the time and space needed to maintain (and check) the copies. So, if the software is refined so that it no longer copies the whole file but just the sensitive sections which are at particular risk from virus attack, it can be made much faster and will occupy less space. Include similar copies of the Master and DOS Boot Sectors and you have a virus-generic disinfection system which will not only disinfect most known viruses, but also any of the more primitive virus types which have not yet been written!

All of the foregoing refers specifically to changes brought about within files by actual virus infection. As mentioned in the report on the NOMENKLATURA virus (*VB*, December 1990, pp. 19-21) corruption introduced by the trigger or payload of a virus is almost invariably incurable.

The 'Brute Force' Approach

The final solution, if you are not sure exactly what is infecting your system, is to reformat your whole system at low level and then reconfigure it from scratch with master program files and data from your latest backups.

This procedure is known as 'brute force disinfection' and was described in *VB*, July 1990, pp. 3-5. If you **do** know what the problem is, such drastic action can usually be avoided. **It is advisable to contact a consultant or company specialising in virus countermeasures before undertaking a low-level format, as alternative procedures may already exist. Before commencing a low-level format, it is recommended that at least one (preferably two) complete data backups are made** Obviously, software should not be backed up at this stage!

Ideally, files should be archived so that data is separated logically from executable items; this greatly facilitates taking backups whether routinely or in an emergency (a detailed study of directory and file structure to assist the backup process will appear in the February edition of *Virus Bulletin*).

Effective software disinfection routines can be found for most of the viruses currently causing infections in the wild. **However, if you are using a commercial disinfection program the best advice would be to verify carefully that a single "cured" program exactly matches its clean master file before commencing general use on other infected files**

Once again, there is no substitute for regular, verified backups of data and configuration files. If such work practices are adopted on a weekly basis, even intentional corruption to data caused by a computer virus will be diagnosed quickly thus limiting the damage wrought. **The importance of regularly verifying the integrity of backed up data (and its capacity to restore correctly) cannot be over-emphasised - otherwise there is the danger of corruption occurring in multiple successive backup generations**

KNOWN IBM PC VIRUSES

This is a list of the known viruses affecting IBM PCs and compatibles, including XTs, ATs and PS/2s. The first part of the list gives aliases and brief descriptions of viruses which have been seen, while the second part lists viruses which have been reportedEach entry consists of the virus group name, its aliases and the virus type (See "Type codes" table). This is followed by a short description (if available) and a 10 to 16 byte hexadecimal pattern which can be used to detect the presence of the virus by the "search" routine of disk utility programs such as *The Norton Utilities* or your favourite disk scanning program. Offset (in hexadecimal) normally means the number of bytes from the virus entry point. For parasitic viruses, the infective length (the amount by which the length of an infected file has increased) is also given.

Type Codes

C = Infects COM files **E** = Infects EXE files **D** = Infects DOS Boot Sector (Logical sector 0 on disk)

M = Infects Master Boot Sector (Track 0, head 0, sector 1 on disk) **N** = Not memory-resident after infection

R = Memory-resident after infection **P** = Companion virus

SEEN VIRUSES

8 Tunes - CER: The virus probably originates in Germany and infects COM and EXE files. The length of the virus code is 1971 bytes. When triggered, it will play one out of eight different tunes. The virus attempts to deactivate two anti-virus programs: Bombsquad and Flushot+.

```
8 Tunes          33F6 B9DA 03F3 A550 BB23 0353 CB8E D0BC ; Offset variable
```

405 - CN: Infects one COM file (on a different disk) each time an infected program is run by overwriting the first 405 bytes. If the length of the file is less than 405 bytes, it will be increased to 405. The virus only infects the current directory and does not recognise a file already infected.

```
405              26A2 4902 26A2 4B02 26A2 8B02 50B4 19CD ; Offset 00A
```

417 - CR: A 417 byte virus, probably of Russian origin. The only text inside the virus is the message "Fuck You".

```
417              C3B4 3FCD 2129 C858 75DD FFE0 B440 EBF3
```

440 - CN: This 440 byte virus is not related to the 440 byte AntiPascal virus. It has not yet been analysed fully.

```
440              A48B FDC3 B104 D3E0 0AC6 FEC1 D3E0 0AC2
```

492 - CR: A Bulgarian virus which has not been analysed. The only available sample seems corrupted.

```
492              2E8B 1E01 0183 C303 B104 D3EB 8CD8 03C3 ; Offset 010
```

516 - CR: This 516 byte Russian virus is the first virus which does not modify the beginning of the programs it infects, but places the jump to the virus code inside the host program.

```
516              431E 53C5 1F46 5F07 8B07 3DFF FF75 F283
```

600 - CR: An encrypted, 600 byte Russian virus.

```
600              BE10 01B9 3200 8A24 80F4 DD88 2446 E2F6
```

696 - CN: A 696 byte Russian virus awaiting analysis.

```
696              3C00 7412 8CC8 B10F D3E0 3D00 8074 07BA
```

707 - CR: A 707 byte Russian virus awaiting analysis

```
707              83C3 0F33 C08E C033 F68C C040 3DFF 0F76
```

711 - CR: A 711 byte Russian virus awaiting analysis.

```
711              C88E C08E D833 C08B F0BF 0000 BB00 01FF
```

800 - CR: Infective length is 800 bytes. The virus code is written into a random location of the infected file. Like Number of the Beast, it uses an undocumented DOS function to obtain the original INT 13H address, and instead of intercepting INT 21H, it intercepts INT 2A, function 82. The virus is encrypted. (*VB* June 90)

```
800              B981 0151 AD33 D0E2 FB59 3115 4747 E2FA ; Offset 00E
```

905 - ER: A Bulgarian virus, still awaiting analysis.

```
905              488E C08E D880 3E00 005A 7415 0306 0300
```

948 - CER: A Russian, 948 byte virus, which seems partially based on the Yankee virus.

```
948             5051 56B9 FF00 FC8B F28A 0446 3C00 E0F9 ; Offset 02d
```

1049 - CER: A 1049 byte Russian virus awaiting analysis.

```
1049            EB10 8CDA 83C2 102E 0316 2000 522E FF36
```

1067 - CR: This virus is closely related to the Ambulance virus, but is still awaiting analysis.

```
1067            018A 5405 8816 0001 B42A CD21 F6C2 0175
```

1077 - CER: This 1077 byte virus infects COM and EXE files, but is unable to infect EXE files larger than 64K.

```
1077            4E01 EACD 21C3 B44F CD21 C351 33C0 3B86
```

1226 - CR: This Bulgarian virus is related to Phoenix, Proud and Evil. As in the case of its relatives, no search pattern is possible.

1260, Stealth - CN: Virus infects COM files, adding 1260 bytes to them. The first 39 bytes contain code used to decrypt the rest of the virus. A variable number of short (irrelevant) instructions are added between the decoding instructions at random in an attempt to prevent virus scanners from using identification strings. An infected file has the seconds field set to 62. No search pattern is possible. (*VB* March 90)

1600 - CER: A 1600 byte Bulgarian virus, reported to be written by the same author as the Nina, Terror and the Anti-Pascal viruses. Many infected programs, including COMMAND.COM will fail to execute when infected.

```
1600            8B35 8936 0001 8B75 0289 3602 01C7 4514
```

2100 - CER: This is a Bulgarian virus, related to the Eddie and Eddie-2 viruses and contains extensive segments of code in common with both. The pattern for Eddie-2 can be found within this virus, but they can be easily differentiated on basis of length.

2144 - CER: A 2144 byte Russian virus, not yet analysed.

```
2144            1E06 33C0 8ED8 FB2E 8B94 1000 EC34 03EE
```

2480 - CR: This virus only spreads if the year is set to 1988, so it is not a serious threat. It is rather long, 2480 bytes, but has not been analysed yet. This virus first appeared in Finland.

```
2480            81C6 0301 01C6 B904 008C C88E C08E D8BF
```

5120 - CEN: This is one of the largest viruses known, 5120 bytes long. When an infected program is run, it will search recursively for EXE and COM files to infect. Infected programs will terminate with an "Access denied" message after 1st June 1992. Parts of the virus seem to have been written in compiled BASIC.

```
5120            40B1 04D3 E88C DB03 C305 1000 8ED8 8C06 ; Offset 026
```

4K, 4096, Frodo, IDF, Israeli Defence Forces - CER: Infective length is 4096 bytes. The virus may occasionally cause damage to files, as it manipulates the number of available clusters, which resultsin crosslinked files. If the virus is memory-resident, it disguises itself from detection by pattern-searching or checksumming programs. Infected systems hang on 22nd September(*VB* May 90)

```
4K              E808 0BE8 D00A E89A 0AE8 F60A E8B4 0A53 ; Offset 239
```

Agiplan - CR: Infective length is 1536. The virus attaches itself to the beginning of COM files. Agiplan has only occurred on one site and may be extinct.

```
Agiplan         E9CC 0390 9090 9090 9C50 31C0 2E38 26DA ; Offset 0
```

AIDS - CN: Not to be confused with the AIDS Trojan, this virus overwrites COM files and is about 12K long. When an infected program is executed, the virus displays "Your computer now has AIDS" and halts the system.

```
AIDS            0600 AE42 6E4C 7203 4600 0004 00A0 1000 ; Offset 2C7F
```

AIDS II - PN: A "companion" virus, 8064 bytes long, which displays a message when it activates. To locate and remove the virus, search for COM files corresponding to EXE files, but marked "Hidden" and located in the same subdirectory.

```
AIDS II         4D5A 8001 1000 7800 2000 9702 9702 6F02 ; Offset 0
```

Alabama - ER: Infective length is 1560 bytes. May cause execution of wrong files and FAT corruption.

```
Alabama         803D C673 0726 C605 CF4F EBF0 26FF 0603
```

Ambulance - CN: The major effect of this virus is to display an ambulance on the screen. The virus is 796 bytes long.

```
Ambulance       0001 8A07 8805 8B47 0189 4501 FFE7 C3E8 ; Offset 016
```

Amoeba - CER: Virus adds 1392 bytes to the length of the infected files. It does not have any known side-effects.

```
Amoeba          CF9C 502E A107 0140 2EA3 0701 3D00 1072 ; Offset 0D1
```

Amstrad - CN: Adds 847 bytes to the front of any COM file in the current directory. The rest contains an advertisment for Amstrad computers. (*VB* June 90). Cancer is a 740 byte long mutation, which infects the same files repeatedly.

```
Amstrad         C706 0E01 0000 2E8C 0610 012E FF2E 0E01 ; Offset 114
```

Amstrad-852 - CN: Almost identical to the original 847 byte mutation, with only a text string changed.

Anthrax - MCER: A multi-partite virus from Bulgaria, which infects the Master Boot Sector, as well as executable files. Infected files usually grow by 1000-1200 bytes.

```
Anthrax          0E1F 832E 1304 02CD 12B1 06D3 E08E C0BF ; Offset 0 in MBR
```

Anti-Pascal - CN: This is a family of 5 Bulgarian viruses, which will overwrite or delete .PAS or .BAK files, if they find no .COM files to infect. All five viruses are rare, even in Bulgaria and fairly simple in structure. The length of the mutations is in the range 400-605.

```
Anti-Pascal (1)  D1E0 D1E0 80E4 0380 C402 8AC4 8BD8 32FF ; Offset variable
Anti-Pascal (2)  21BE 0001 5A58 FFE6 50B4 0E8A D0CD 2158 ; Offset variable
```

Armagedon - CR: A 1079 byte virus from Greece, which interferes with the serial port. It will produce control strings for Hayes-compatible modems, dialling number 081-141 (speaking clock in Crete). Virus name is spelt with a single 'd'.

```
Armagedon        018C CBEA 0000 0000 8BC8 8EDB BE00 01BF ; Offset 3F0
```

Attention - CR: A Russian, 394 byte virus. The virus has some code in common with the "Best Wishes" virus, which is possibly written by the same author. Infective length is 393 bytes and only files longer than 786 bytes are infected. Disk writing is done by outputting directly to hardware via port 3F2H.

```
Attention        B000 8BDA B501 433A 0775 FB4B 4B81 275F
```

Bebe - CN: A Russian, 1004 byte virus.

```
Bebe             B104 D3EB 240F 3C00 7401 4389 1E0C 00C7
```

Beijing, Bloody! - MR: A primitive 512-byte virus. On 129th boot and every sixth boot thereafter, the virus will display the message ''Bloody! Jun. 4, 1989''. The virus is believed to be a protest against the Tiananmen Square massacre.

```
Beijing          80FC 0272 0D80 FC04 7308 80FA 8073 03E8 ; Offset 01F
```

Best Wishes - CR: A 1024 byte Russian virus containing the message "This programm ... With Best Wishes!". Many programs, including COMMAND.COM will not work properly if infected with this virus.

```
Best Wishes      4C00 268C 1E4E 0007 1FB8 0400 8BF5 81EE
```

Black Monday - CER: This virus was first isolated in Fiji, but may have been written elsewhere. It adds 1055 bytes to infected files. The name is derived from the following message "Black Monday 2/3/90 KV KL MAL". Infected EXE files cannot be disinfected, as the virus will overwrite a few bytes at the end of the file.

```
Black Monday     8B36 0101 81C6 0501 8B04 8B5C 02A3 0001
```

Blood - CN: A simple virus from Natal, South Africa. The 418 byte virus does nothing of interest, except from replicating.

```
Blood            1E0E 1FB4 19CD 2150 B202 B40E CD21 B41A ; Offset 07F
```

Brain, Ashar, Shoe - DR: Consists of a bootstrap sector and 3 clusters (6 sectors) marked as bad in the FAT. The first of these contains the original boot sector. In its original version it only infects 360K floppy disks and occupies 7K of RAM. It creates a label "(c) Brain" on an infected disk. There is a variation which creates a label "(c) ashar".

```
Brain            FBA0 067C A209 7C8B 0E07 7C89 0E0A 7CE8 ; Offset 157
```

Burger - CN: Just like the 405 virus, this primitive 560 byte virus overwrites the infected files, which makes it easily detectable. Several mutations with slightly different lengths are known.

```
Burger (1)       B447 0401 508A D08D 3646 02CD 2158 B40E; Offset 01B
Burger (2)       CD21 B43E CD21 2E8B 1E00 E081 FB90 9074 ; Offset variable
```

Carioca - CR: This virus adds 951 bytes to the end of infected programs, but it has not been analysed yet.

```
Carioca          01FC F3A4 B800 0150 C32E 8B1E 0301 81C3
```

Cascade, Fall, Russian, Hailstorm - CR: This encrypted virus attaches itself to the end of COM files, increasing their length by 1701 or 1704 bytes. The encryption key includes the length of the infected program, so infected files of different lengths will look different. After infection it becomes memory-resident and infects every COM file executed, including COMMAND.COM. The original version will produce a "falling characters" display if the system date is between 1st October and 31st December 1988. The formatting version will format the hard disk on any day between 1st October and 31st December of any year except 1993. Both activations occur a random time after infection with a maximum of 5 minutes.(*VB* Sept 89)

```
Cascade (1) 01   0F8D B74D 01BC 8206 3134 3124 464C 75F8 ; Offset 012, 1701 bytes, Falling characters
Cascade (1) 04   0F8D B74D 01BC 8506 3134 3124 464C 75F8 ; Offset 012, 1704 bytes, Falling characters
Cascade (1) Y4   FA8B CDE8 0000 5B81 EB31 012E F687 2A01 ; Offset 000, 1704 bytes, Falling characters
Cascade format   0F8D B74D 01BC 8506 3134 3124 464C 77F8 ; Offset 012, 1704 bytes, Formats hard disk
```

Casper - CN: This virus was written by Mark Washburn and uses the same encryption method as his 1260 virus. The infective length is 1200 bytes.The virus sets the seconds field to 62. The source code for this virus has been widely circulated;it includes a 'manipulation task' (payload) which will format cylinder 0 of the hard disk. No search pattern is possible.

Christmas in Japan - CN: 600 byte Taiwanese virus. Activates on 25th December and displays "A merry christmas to you".

```
Christmas Japan     32E4 CF8A 1446 80F2 FE74 06B4 06CD 21EB ; Offset 23F
```

Christmas Tree, Father Christmas, Choinka - CN: This is a Polish 1881 byte version of the Vienna virus, which only activates from 19th December to the end of the year and displays a "Merry Christmas" message. Damage to files has been reported, but not confirmed. This virus is also detected by the Vienna (4) string.

```
Christmas Tree      CD21 81FA 130C 7308 81FA 0101 7202 EB0E
```

Cookie - CER: This 2232 byte virus may display the message "I want a COOKIE!", and wait for input from the user. It is closely related to the Syslock/Macho/Advent viruses, and is identified by the Syslock string.

Dark Avenger - CER: The virus infects when a file is opened and closed as well as when it is executed. This means that a virus-scanning program will cause it to infect every program scanned. Infective length is 1800 bytes. It only infects if a program is at least 1775 bytes long and it may overwrite data sectors with garbage. There is a mutation which extends the file by 2000 bytes.(*VB* Feb 90)

```
Dark Avenger        A4A5 8B26 0600 33DB 53FF 64F5 E800 005E ; Offset variable
```

Datacrime - CN: The virus attaches itself to the end of a COM file, increasing its length by 1168 or 1280 bytes. On execution of an infected program, the virus searches through the full directory structure of drives C, D, A and B for an uninfected COM file which will be infected. Files with 7th letter D will be ignored (including COMMAND.COM). If the date is on or after 13th October of any year, the first 9 tracks of the hard disk will be formatted. The format is low level after displaying the message:

```
DATACRIME VIRUS
RELEASED: 1 MARCH 1989
```

This message is stored in an encrypted form in the virus.(*VB* Aug 89)

```
Datacrime (1)       3601 0183 EE03 8BC6 3D00 0075 03E9 0201 ; Offset 002, 1168 bytes
Datacrime (2)       3601 0183 EE03 8BC6 3D00 0075 03E9 FE00 ; Offset 002, 1280 bytes
```

Datacrime II - CEN: This encrypted virus attaches itself to the end of a COM or EXE file, increasing their length by 1514 bytes. The virus searches through the full directory structure of drives C, A and B for an uninfected COM or EXE file. It ignores any file if the second letter is B. If the date is on or after 13th October of any year, but not a Monday, a low level format of the first 9 tracks will be done on the hard disk after displaying the message: "DATACRIME II VIRUS" which is stored in an encrypted form. Datacrime IIB displays the message "* DATACRIME *".(*VB* Aug 90)

```
Datacrime II        2E8A 072E C605 2232 C2D0 CA2E 8807 432E ; Offset 022, 1514 bytes
Datacrime IIB       2BCB 2E8A 0732 C2D0 CA2E 8807 43E2 F3 ; Offset 01B
```

Datalock - CER: The name of this 920 byte virus is included at the end of infected programs, but its effect are not known yet.

```
Datalock            C31E A12C 0050 8CD8 488E D881 2E03 0080
```

dBASE - CR: Transposes bytes in dBASE (DBF) files. Creates the hidden file BUGS.DAT in the root directory of drive C and generates errors if the absolute difference between the month of creation of BUGS.DAT and the current month is greater or equal to 3. Infective length is 1864 bytes. The destroy version destroys drives D to Z when the trigger point is reached.(*VB* Dec 89)

```
dBASE               50B8 0AFB CD21 3DFB 0A74 02EB 8A56 E800 ; Offset 636, 1864 bytes
dBASE destroy       B900 01BA 0000 8EDA 33DB 50CD 2658 403C ; Offset 735, 1864 byte
```

DBF Blank - CER: This virus waits for a dBASE (DBF) file to be opened and returns a blank record once every 20 disk reads. Only one DBF file is affected at a time. Infective length is 1075 bytes.

```
DBF Blank           33C0 8ED8 813E 8801 564F 1F75 212E 813C
```

December 24th - ER: A mutation of the Icelandic (3) virus. It will infect one out of every 10 EXE files run, which grow by 848-863 bytes. If an infected file is run on December 24th, it will stop any other program from running and display the message "Gledileg jol" (Merry Christmas in Icelandic).

```
December 24th       C606 7E03 FEB4 5290 CD21 2E8C 0645 0326 ; Offset 044
```

Den Zuk, Search - DR: The majority of the virus is stored in a specially formatted track 40, head 0, sectors 33 to 41. When Ctrl-Alt-Del is pressed, the virus intercepts it and displays "DEN ZUK" sliding in from the sides of the screen. This does not happen if KEYBUK or KEYB is installed. Den Zuk will remove Brain and Ohio and replace them with copies of itself.

```
Den Zuk (1)         FA8C C88E D88E D0BC 00F0 FBE8 2600 33C0 ; Offset 02C
Den Zuk (2)         FA8C C88E D88E D0BC 00F0 FBB8 787C 50C3 ; Offset 02C
```

Destructor - CER: A 1150 byte Bulgarian virus containing the string "DESTRUCTOR V4.00 (c) 1990 by ATA".

```
Destructor          5255 FBCB 3D00 4B74 1980 FC3D 740F 80FC
```

Devil's Dance - CR: A simple virus which infects COM files, adding 951 bytes at the end of infected files. The virus is believed to have originated in Spain or Mexico. It monitors the keyboard and will destroy the FAT after 5000 keystrokes.

```
Devil's Dance       B800 0150 8CC8 8ED8 8EC0 C306 B821 35CD ; Offset 011
```

Diamond, 1024 - CER: A Bulgarian virus, possibly written by the person calling himself (?) "Dark Avenger". This virus may be an earlier version of the Eddie virus. No side-effects or activation dates have been found. Diamond-B is a minor mutation.

```
Diamond          00B4 40CD 2172 043B C174 01F9 C39C 0EE8 ; Offset 170
```

Dir - CR: A 691 byte Bulgarian virus, which only infects files when the DIR command is issued. No other effects have been found.

```
Dir              CD26 0E1F 580E 1FBE 0001 56C3 0E0E 1F07 ; Offset 04A
```

Diskjeb - CER: A disk-corrupting virus with an infective length of 1435 bytes (COM) and 1419 bytes (EXE). Only infects COM files longer than 1000 bytes and EXE files longer than 1024 bytes. In October, November and December disk writes will be intercepted and corrupted. A possible mutation of the Tenbyte virus.

```
Diskjeb          5351 061E 9C8C C88E D8E8 5D00 803E 4903 ; Offset 4E8
```

Disk Killer, Ogre - DR: The virus infects floppy and hard disks and if the computer is left on for more than 48 hours, it will encrypt the contents of the bootable disk partition. The infection of a disk occurs by intercepting a disk read - INT 13H function 2. When the virus triggers, it displays the message "Disk Killer — Version 1.00 by Ogre Software, 04/01/1989. Warning !! Don't turn off the power or remove the diskette while Disk Killer is Processing!". (*VB* Jan 90)

```
Disk Killer      2EA1 1304 2D08 002E A313 04B1 06D3 E08E ; Offset 0C3
Disk Killer 2    7423 2E3A 16F4 0175 EE2E 3A36 F501 75E7
```

Do-nothing - CR: A badly-written virus from Israel that assumes a 640K system.

```
Do nothing       8CCA 8EDA BA00 988E C2F3 A41E B800 008E ; Offset 020
```

Dot Killer - CN: This 944 byte Polish virus will remove all dots (.) from the screen when they are typed. The effect can be disabled by typing a caret '^'. Seconds field is set to 62. Files set to Read-Only will not be infected.

```
Dot Killer       582E A301 0158 2EA2 0001 B800 01FF E0B8
```

Durban, Saturday 14th - CER: Adds 669 bytes to the end of infected files. On any Saturday 14th the first 100 logical sectors of drives C, then B and then A are overwritten.

```
Durban           B911 00A4 E2FD B4DE CD21 80FC DF74 47C6 ; Offset 02F
```

Dyslexia, Solano - CR: Virus adds 1991 bytes in front of the infected file and 9 bytes at the end. Occasionally transposes two adjacent characters on the screen.

```
Dyslexia         B4C0 CD21 3D34 1275 0E2E 8B0E 0301 1E07
```

Eddie-2, 651 - CER: A non-destructive virus from Bulgaria. It marks infected files with a value of 62 in the seconds field of the timestamp, which makes them immune from infection by Vienna or Zero Bug. Infected files grow by 651 bytes, but this will not be seen if a DIR command is used - the virus intercepts the find-first and find-next functions, returning the correct (uninfected) length(*VB* June 90)

```
Eddie-2          D3E8 408C D103 C18C D949 8EC1 BF02 00BA ; Offset 02D, 651 bytes
```

E.D.V. - DR: E.D.V. marks infected disks with "EV" at the end of the boot sector and stores the original boot sector code in the last sector of the last track on 360K disks, just like the Yale virus. Program crashes and data loss have been reported on infected systems.

```
E.D.V.           0C01 5083 EC04 B800 01CF B601 B908 2751 ; Offset 0C1
```

Evil - CR: This is a close relative of the Bulgarian Phoenix virus, but is shorter, 1701 bytes instead of 1704. It uses the same encryption method, which makes the extraction of a search pattern impossible.

Fellowship - ER: This 1019 byte virus attaches itself to the end of EXE files, damaging them by overwriting the last 10 bytes or so. Other effects are being analysed.

```
Fellowship       BAF5 02E8 3A00 B60A E84A 00BA 1403 E82F ; Offset 389
```

Filler - DR: A Hungarian virus with unknown effects.

```
Filler           CD12 BB40 00F7 E32D 0010 8EC0 BA00 00EB ; Offset 074
```

Fish 6 - CER: A partial mutation of 4K having an infective length of 3584 bytes. The virus is encrypted and the decryption routine is so short that it is impossible to extract a hex pattern longer than 14 bytes. The virus seems to activate in 1991, but the exact effects are yet unknown.

```
Fish 6           E800 005B 81EB A90D B958 0D2E 8037    ; Offset 0
```

Flash - CER: This 688 byte virus is awaiting analysis.

```
Flash            005E 8BDE 81C3 0F00 B000 FAD5 0A88 07EB ; Offset 007
```

Flip - MCER: The primary effect of this 2343 byte virus is to "flip" the screen by rotating it through 90 degrees. The virus is encrypted and self-modifying. An infected file has the seconds field set to 62. No search pattern is possible for COM/EXE files. Search pattern will be found in the Master Boot Sector. (*VB* Sept 90)

```
Flip (boot)      33DB 33FF 8EC3 2629 0613 04CD 12B1 06D3 ; in MBS          ; Offset 02E
```

Form - BR: A boot sector virus from Switzerland infecting hard disks and floppy disks. On the 24th day of every month the virus produces a small delay when keys are pressed.

```
Form            B106 D3E0 8EC0 33FF B9FF 00FC F3A5 06B8 ; Offset 074
```

Freeze - CR: A 1024 byte virus which makes the computer "hang" at random intervals.

```
Freeze          4545 5A45 B8EF EFCD 213D FEFE B800 0074 ; Offset 002
```

Fu Manchu - CER: The virus attaches itself to the beginning of a COM file or to the end of an EXE file. Infective length is 2086 bytes (COM) and 2080 (EXE). It is a rewritten version of the Jerusalem virus, but the marker is "rEMHOr" and the preceding "sU" is "sAX" (Sax Rohmer, creator of Fu Manchu). After installing itself as memory-resident, it will infect any COM or EXE file, except COMMAND.COM. EXE files are infected only once, unlike the original Jerusalem. One in sixteen times on infection a timer is installed, which will trigger a display "The world will hear from me again" after a random number of half-hours (max. 7.5 hours). The machine then reboots. The same message is also displayed on pressing Ctrl-Alt-Del, but the virus does not survive the reboot. If the date is after 1st August 1989, the virus monitors the keyboard buffer and adds derogatory comments to the names of politicians (Thatcher, Reagan, Botha and Waldheim), overstrikes two four-letter words, and displays "virus 3/10/88 - latest in the new fun line!" if "Fu Manchu" is typed. All messages are encrypted. (*VB* July 89)

```
Fu Manchu       FCB4 E1CD 2180 FCE1 7316 80FC 0472 11B4 ; Offset 1EE, 2086 bytes COM, 2080 bytes EXE
```

GhostBalls - CN: A strain of Vienna virus. Seconds field changed to 62, as in Vienna. Infective length is 2351 bytes and the virus attaches itself to the end of the file. When run, it will infectCOM files and try to place a modified copy of the Italian virus into boot sector of drive A. This copy of Italian runs on 286 machines but is non-infective. Virus contains text "GhostBalls, Product of Iceland".

```
GhostBalls      AE75 EDE2 FA5E 0789 BC16 008B FE81 C71F ; Offset 051
```

Groen Links, GrLkDos - CER: A 1888 byte version of Jerusalem, which originated in the Netherlands. Every 30 minutes it will play the tune "Stem op Groen Links", or "Vote Green Left". This virus is detected by the Jerusalem (USA) string.

Guppy - CR: A very simple 152 byte virus. It does nothing but replicate, but many programs, including COMMAND.COM will fail to execute if infected.

```
Guppy           521E B802 3DCD 2193 E800 005E 0E1F B43F ; Offset 045
```

Hallochen - CER: A virus which reputedly originated in West Germany. It contains two text strings (o in Hallochen is character code 148 decimal):

```
Hallochen !!!!!!, Here I'm..
Acrivate Level 1..
```

The virus will not infect "old" files. If the value of the month or year fields in the time stamp is different from the current date, the file will not be infected. The virus will only infect files longer than 5000 bytes, increasing their length by 2011 bytes.

```
Hallochen       EB8C C903 D98E D3BC DB08 53BB 2E00 53CB ; Offset 01E, 2011 bytes
```

Hymn - CER: A Russian, 1865 byte virus related to the "Eddie" (Dark Avenger) virus, and the "Murphy" viruses as well.

```
Hymn            FF64 F500 07E8 0000 5E83 EE4C FC2E 81BC
```

Icelandic, Saratoga - ER: The virus attaches itself at the end of an EXE file and after becoming memory-resident, it will infect only one in ten (one in two for the Icelandic (2) mutation) programs executed. When a program is infected, the disk is examined and if it has more than 20 MBytes, one cluster is marked as bad in the first copy of the FAT. There is a mutation which does not flag clusters. Version (1) will not infect the system unless INT 13H segment is 0700H or F000H, thus avoiding detection by anti-virus programs which hook into this interrupt. Version (3) does not flag clusters and bypasses all interrupt-checking programs.

```
Icelandic (1)   2EC6 0687 020A 9050 5351 5256 1E8B DA43 ; Offset 0C6, 656 bytes
Icelandic (2)   2EC6 0679 0202 9050 5351 5256 1E8B DA43 ; Offset 0B8, 642 bytes
Icelandic (3)   2EC6 066F 020A 9050 5351 5256 1E8B DA43 ; Offset 106, 632 bytes
```

Internal - EN: Infective length is 1381 bytes. Virus contains the string:

```
INTERNAL ERROR 02CH.
PLEASE CONTACT YOUR HARDWARE MANUFACTURER IMMEDIATELY !
DO NOT FORGET TO REPORT THE ERROR CODE !

Internal        1E06 8CC8 8ED8 B840 008E C0FC E858 0480 ; Offset 0B1
```

Italian, Pingpong, Turin, Bouncing Ball, Vera Cruz - DR: The virus consists of a boot sector and one cluster (2 sectors) marked as bad in the first copy of the FAT. The first sector contains the rest of the virus while the second contains the original boot sector. It infects all disks which have at least two sectors per cluster and occupies 2K of RAM. It displays a single character "bouncing ball" if there is a disk access during the one-second interval in any multiple of 30 minutes on the system clock. The original version will hang when run on an 80286 or 80386 machine, but a new version has been reported which runs normally. If a warm boot is performed after the

machine hangs, an uninfected disk will still become infected.(*VB* Nov 89)

```
Italian-Gen        B106 D3E0 2DC0 078E C0BE 007C 8BFE B900 ; Offset 030
Italian            32E4 CD1A F6C6 7F75 0AF6 C2F0 7505 52E8 ; Offset 0F0
```

Itavir - EN: When the virus activates, it will write random data to all I/O ports causing unpredictable behaviour such as screen flicker, hissing from the loudspeaker etc. Infective length is 3880 bytes.

```
Itavir             83C4 025A 595B 5850 5351 52CD 2672 0D83 ; Offset 198
```

Jerusalem, PLO, Friday the 13th, Israeli - CER: The virus attaches itself to the beginning of a COM file or at the end of an EXE file. When an infected file is executed, the virus becomes memory-resident and will infect any COM or EXE program run, except COMMAND.COM. COM files are infected only once, while EXE files are re-infected every time that they are run. Infective length is 1813 bytes (COM) and 1808 bytes (EXE). The virus finds the end of EXE files from the information in the file header, and if this is less than the actual file length, the virus will overwrite part of the file. After the system has been infected for 30 minutes, row 5 column 5 to row 16 column 16 on the screen are scrolled up two lines, creating a "black window". The system then slows down, due to a time-wasting loop installed on each timer interrupt. If the system is infected when the date is set to 13th of any month which is also a Friday, every program run will be deleted. (*VB* July 89)

```
Jerusalem          03F7 2E8B 8D11 00CD 218C C805 1000 8ED0 ; Offset 0AC, 1813 BYTES COM, 1808 bytes EXE
Jerusalem-USA      FCB4 E0CD 2180 FCE0 7316 80FC 0372 11B4 ; Offset 095
```

Minor Jerusalem mutations matching the Jerusalem search pattern Anarkia: Virus signature is changed from 'sURIV' to 'ANARKIA'. **Anarkia-B**: Minor mutation of Anarkia. **Mendoza**: Another minor mutation of Anarkia. **PSQR**: Mutation with the signature changed to 'PSQR'. The infective length is 1715 (COM) and 1720 bytes (EXE).

```
PSQR               FCB8 0FFF CD21 3D01 0174 3B06 B8F1 35CD ; Offset 071
```

Jo-Jo - CR: This is a non-encrypted version of Cascade with the encryption code patched out and a few other changes made.

```
Jo-Jo              B800 F08E C0BF 08E0 813D 434F 751B 817D ; Offset 0D2
```

Jocker: An overwriting virus from Poland, written in some high-level language, probably Pascal. The sample only replicates after the file name is changed to WABIKEXE.EXE. Wabik is a Polish word meaning 'decoy' or 'allure'.

```
Jocker             89E5 81EC 0001 BF00 000E 57BF 401B 1E57 ; Offset 00B
```

Joker-01 - CR: A huge, 29233 byte virus of Polish origin.

```
Joker-01           8CC2 4A8E C28C DA4A 8EDA 5A90 26A1 0300
```

Joshi - MR: This virus from India displays the message 'Type "Happy Birthday Joshi"' on 5th January of every year. Unless the user enters the text verbatim, the computer will hang. The virus traps disk reads and any program trying to discover it while the virus is active in memory, will not locate it. Survives warm boot.(*VB* Dec 90)

```
Joshi              FA8C C88E D88E D0BC 00F0 FBA1 1304 B106 ; Offset 021
```

July 13th - ER: This encrypted virus activates on 13th July, but its exact effects have not yet been determined. It is 1201 bytes long.

```
July 13th          2EA0 1200 3490 BE12 00B9 B104 2E30 0446 ; Offset variable
```

Kamikaze- EN: This overwriting virus from Bulgaria is written in Turbo Pascal, and is fairly large, 4031 bytes. Like other similar viruses it is not a threat.

```
Kamikaze           8EDA 8C06 3E00 33ED 8BC4 0513 00B1 04D3 ; Offset 3CD
```

Kemerovo - CN: A Russian, 257 byte virus. Some infected programs fail to execute properly, but no other effects are known.

```
Kemerovo           0400 89C7 B904 00A4 E2FD 89D7 29D3 81EB
```

Kennedy - CN: A simple COM infecting virus, probably originating from Sweden. When an infected file is run, it will infect a single COM file in the current directory, expanding it by 333 bytes at the end. The virus activates on three dates: 6th June, 18th November and 22nd November and displays the message

```
Kennedy er dod - lange leve "The Dead Kennedys"
```

```
Kennedy            E817 0072 04B4 4FEB F38B C505 0301 FFE0 ; Offset 035
```

Keypress, Turku, Twins - CER: This virus was discovered at the same time in Finland, USSR and Bulgaria, which makes its origin somewhat uncertain. It will infect COM and EXE files, but the length of the virus code is different, 1232 and 1472 bytes, respectively. After being resident for some time the virus will interfere with the keyboard, causing keys to "repeat".

```
Keypress           7405 C707 0100 F9F5 1FC3 F606 1801 0174
```

Korea, NJH - DR: A simple boot sector virus with no side-effects. It may cause damage to data, as the original boot sector is always written to sector 11. There are two versions, probably due to two different assemblers being used.

```
Korea              C08E D88E D0BC F0FF FBBB 1304 8B07 4848 ; Offset 009
```

Lehigh - CR: The virus only infects COMMAND.COM. It is 555 bytes long and becomes memory-resident when the infected copy is run. If a disk is accessed which contains an uninfected COMMAND.COM, the copy is infected. A count of infection generation is kept

inside the virus, and when it reaches 4 (or 10 in a mutated version), the current disk is trashed each time a disk is infected, provided that (a) the current disk is either in the A drive or B drive, (b) the disk just infected is either the A drive or B drive and (c) the disk just infected is not the current one. The trashing is done by overwriting the first 32 sectors following the boot sector. Infection changes the date and time of COMMAND.COM.

```
Lehigh          8B54 FC8B 44FE 8ED8 B844 25CD 2106 1F33 ; Offset 1EF
```

Leprosy-B - CER: A 666 byte overwriting virus, which is easily detected, as infected programs do not run normally, but instead display a message announcing the virus.

```
Leprosy-B       8A27 3226 0601 8827 4381 FBCB 037E F1C3 ; Offset 021
```

Liberty - CER: A virus from Indonesia with an infective length of 2857 bytes, but a 2867 byte mutation is also known. No harmful effects have been reported, but the virus is awaiting disassembly.

```
Liberty         0174 031F 595B 5053 5152 1E06 1E0E 1FE8 ; Offset 080
```

Lozinsky - CR: A Russian, 1023 byte virus, which uses a simple encryption algorithm.

```
Lozinsky        FCBF 2000 03FE B9D0 032E 3005 47E2 FAB8 ; Offset 013
```

LoveChild - CEN: Infective length is 467 bytes. Contains string "LoveChild in reward for software sealing."[sic] Sample obtained does not replicate under test conditions.

```
LoveChild       33C0 8EC0 E800 005E 8BEE BFE0 01FC 2681
```

Macho - CEN: Swaps every string "MicroSoft" with "MachoSoft" on the hard disk. Searches 20 sectors at a time, storing the last sector searched in IBMNETIO.SYS which is marked hidden and system. After searching the last sector it starts again. This will only happen after 1st January 1985 and if the environment variable VIRUS is not set to OFF. Infective length is 3550 to 3560 bytes. Random directory search for uninfected files. Infects COMMAND.COM. This virus is closely related to Syslock.

```
Macho           5051 56BE 5900 B926 0890 D1E9 8AE1 8AC1 ; Offset ?
```

MG - CR: A simple, 500 byte Bulgarian virus.

```
MG              AA1F 1E07 585E 1EBB 0001 53CB 3D04 4B74 ; Offset 086
```

MG-3 - CR: A 500 byte Bulgarian virus, reported to be written by the same author as the MG virus.

```
MG-3            C43E 0600 B0EA 49F2 AE26 C43D 83EF DFEA
```

MGTU - CN: A simple, 273 byte Russian virus.

```
MGTU            03F8 BE00 018B 0589 048B 4502 8944 02B8 ; Offset 0F8
```

Microbes - DR: An Indian virus the effects of which are not fully known, except that booting from an infected disk has been reported to cause some computers to "hang".

```
Microbes        042D 0400 A313 04B1 06D3 E08E C006 C706 ; Offset 014
```

Mistake, Typoboot, Typo - DR: Exchanges letters for phonetically similar ones (for example "C" and "K") while they are being output to the printer. Reportedly written in Israel. A mutation of the Italian virus with about 35% of the code rewritten. The boot sector is almost identical to the Italian.

```
Mistake         32E4 CD1A 80FE 0376 0A90 9090 9090 52E8 ; Offset 0F0
```

MIX1 - ER: The virus infects only EXE files, attaching itself to the end. When an infected program is run, the virus will copy itself to the top of the free memory. Some programs may overwrite this area, causing the machine to crash. The virus traps printer and asynch interrupts and corrupts traffic by substituting characters. 50 minutes after infection, the virus alters Num Lock and Caps Lock keyboard settings. 60 minutes after infection, a display similar to the Italian virus (bouncing ball) will be produced. The virus will infect every tenth program run. Infected files always end in "MIX1" and the infective length of MIX1 is 1618 to 1633 bytes and MIX1-2 1636 to 1651 bytes. (*VB* Dec 89)

```
MIX1            B800 008E C026 803E 3C03 7775 095F 5E59 ; Offset 02E
MIX1-2          B800 008E C0BE 7103 268B 3E84 0083 C70A ; Offset 02A
```

MLTI - CR: This 830 byte Russian virus contains the following text, whichrefers to the "Eddie" (Dark Avenger) virus. "Eddie die somewhere in time! This programm was written in the city of Prostokwashino (C) 1990 RED DIAVOLYATA Hello! MLTI!''

```
MLTI            5B73 05B8 0001 50C3 83FC E072 F62E C747
```

Monxla, Time - CN: A 939 byte mutation of the Vienna virus, which activates on the 13th day of any month and then damages programs, instead of just infecting them.

```
Monxla          8B07 5B8E C0BF 0000 5E56 83C6 1AAC B900
```

Murphy - CER: Two versions exist. One produces a click from the loudspeaker when any DOS functions are called while the other may produce the bouncing-ball effect when the user enters ROM BASIC. The virus will only activate between 10:00 and 11:00 a.m.

```
Murphy 1        1EE8 0000 B859 4BCD 2172 03E9 2801 5E56 ; Offset variable
```

```
Murphy 2          1EE8 0000 B84D 4BCD 2172 03E9 2601 5E56 ; Offset variable
```

Music Bug - DR:

```
Music Bug         08FC F3A5 06B8 0002 50CB 5053 5152 2EA3
```

New Zealand, Stoned, Marijuana - MR: The virus consists of a boot sector only. It infects all disks and occupies 2K of RAM. On floppy disks, sector 0 is infected, while on the hard disks the physical sector 0 (Master boot sector) is infected. The original boot sector is stored in track 0 head 1 sector 3 on a floppy disk and track 0 head 0 sector 2 on a hard disk. The boot sector contains two character strings: "Your PC is now Stoned!" and "LEGALISE MARIJUANA" but only the former one is displayed, once in eight times, and only if booted from floppy disk. The version (2) stores the original boot sector at track 0 head 0 sector 7 on a hard disk. The second string is not transferred when a hard disk is infected. A mutation displays the message "Your PC is now Sanded". A mutation has been reported in Australia which also displays "LEGALISE MARIJUANA".(*VB* May 90)

```
New Zealand (1)   0400 B801 020E 07BB 0002 B901 0033 D29C ; Offset 043
New Zealand (2)   0400 B801 020E 07BB 0002 33C9 8BD1 419C ; Offset 041
```

Nina - CR: Yet another small virus from Bulgaria. This one is 256 bytes long.

```
Nina              03F7 B900 01F3 A458 1EBD 0001 55CB 5858 ; Offset 069
```

NOMENKLATURA - CER: Infective length is 1024 bytes, and only files longer than 1024 bytes are infected. The virus infects on executing a program or opening a file, which means that a virus scanning program will infect all files on the system if the virus is resident in memory. The virus scrambles the FAT on a random basis.(*VB* Dec 90)

```
NOMENKLATURA      B8AA 4BCD 2173 785E 5606 33C0 8ED8 C41E ; Offset 2DD
```

Number of the Beast, 666, V512 - CR: An advanced virus from Bulgaria, only 512 bytes long. The length of the file does not appear to increase since the virus overwrites the first 512 bytes of the programs it infects with itself, storing the original 512 bytes in the unused space of a disk cluster, after the logical end of file. Three variants have now appeared.(*VB* May 90, June 90)

```
Number of Beast   5A52 0E07 0E1F 1EB0 5050 B43F CBCD 2172 ; Offset 0A3
Number of Bea 1   B800 3DCD 2193 5A52 0E1F 1E07 B102 B43F ; Offset variable
Number of Bea E   1607 8BD6 B102 B43F CD21 8AD1 86CD BFFE
Number of Bea F   5A52 0E1F 1E07 06B0 5050 B43F CBCD 2172
```

Ohio - DR: Boot sector virus, probably an older version of Den Zuk.

```
Ohio              FAFA 8CC8 8ED8 8ED0 BC00 F0FB E845 0073 ; Offset 02B
```

Old Yankee - EN: This is the first of the viruses which play the "Yankee Doodle Dandy". It only infects EXE files, increasing their length by 1961 bytes. When an infected program is run, it will infect a new file and then play the melody.(*VB* June 90)

```
Old Yankee        03F3 8CC0 8904 0E07 53B8 002F CD21 8BCB ; Offset 009
```

Oropax, Music virus - CR: The length of infected files increases between 2756 & 2806 bytes and their length becomes divisible by 51. 5 minutes after the infection, the virus plays three different tunes at 7-minute intervals. Does not infect COMMAND.COM.

```
Oropax            06B8 E033 CD21 3CFF 7423 8CCE 8EC6 8B36
```

Parity - CN: A Bulgarian 441 byte virus which may emulate a memory failure when an infected program is run, displaying the message "PARITY CHECK 2" and halting the computer.

```
Parity            40B9 B901 BA00 0103 D7CD 21B8 0157 8B8D
```

Pentagon - DR: The virus consists of a boot sector and two files. The sample obtained does not work, but it contains the code which would survive a warm boot (Ctrl-Alt-Del). It could only infect 360K floppy disks, and will look for and remove Brain from any disk it infects. It occupies 5K of RAM.

```
Pentagon          8CC8 8ED0 BC00 F08E D8FB BD44 7C81 7606; Offset 037
```

Perfume - CR: The infected program will sometimes ask the user for input and not run unless the answer is 4711 (name of a perfume). In some cases the question is "Bitte gebe den G-Virus Code ein", but in other cases the message has been erased. The virus will look for COMMAND.COM and infect it. Infective length is 765 bytes.

```
Perfume           FCBF 0000 F3A4 81EC 0004 06BF BA00 57CB ; Offset 0AA
```

Phoenix, P1 - CR: This Bulgarian virus is 1701 bytes long, but a mutation, 1704 bytes long, has also been reported. Despite the identical lengths, they are not related to the Cascade viruses. These viruses use advanced encryption and no search pattern is possible.

Piter - CR: A Russian, 529 byte virus.

```
Piter             8E1E 2C00 33F6 AC0A 0475 FB83 C603 8BD6 ; Offset 092
```

Pixel - CN: The Pixel viruses are nearly identical to the Amstrad virus but shorter: 345 and 299 bytes. No side-effects occur until the 5th generation, at which stage there is a 50 % chance that the following message will appear when an infected program is executed:

```
Program sick error: Call doctor or buy PIXEL
for cure description
```

```
Pixel (1)          0E1F 2501 0074 4CBA D801 B409 CD21 CD20 ; Offset 0C8, 354 bytes
Pixel (2)          BA9E 00B8 023D CD21 8BD8 061F BA2B 01B9 ; Offset 033, 299 bytes
Pixel (3)          0001 0001 2E8C 1E02 018B C32E FF2E 0001
```

Plastique, AntiCAD - CER: This is a family of 5 viruses from Taiwan, which are based on the Jerusalem virus, but with considerable modifications. This group of viruses includes a 2900 byte mutation, another which is 3012 bytes, and three different mutations 4096 bytes long, one of which is also known as "Invader".The Plastique virus triggers when ACAD.EXE(the AUTOCAD~ design program) is executed. Drives A: and B: are checked for the presence of a diskette;if found the virus overwrites head 0 of all tracks with the contents of memory from address 0000:0000. Then an 'explosion' routine(a noise generated through the speaker approximately every 4.5 minutes) commences. The first and second fixed disks are overwritten on all heads and tracks.(*VB* Jan 91)

```
Plastique (1)      B840 4BCD 213D 7856 7512 B841 4BBF 0001 ; Offset 000
Plastique (2)      C08E D8A1 1304 B106 D3E0 8ED8 33F6 8B44
```

Polimer - CN: A 512 byte Hungarian virus, which only displays the following message when an infected program is executed: "A le' jobb kazetta a Polimer kazetta ! Vegye ezt !"

```
Polimer            8CD8 0500 108E D8B4 40CD 218C D82D 0010 ; Offset 0F5
```

Polish 217 - CR: A simple 217 byte virus from Poland, which noes nothing but replicate.

```
Polish 217         D201 BF00 01B9 0300 F3A4 5EB4 4EBA C901
```

Pretoria, June 16th - CN: Overwrites the first 879 bytes of infected files with a copy of itself, and stores the original 879 bytes at the end of the file. When an infected program is executed, the virus searches the entire current drive for COM files to infect. On 16th June the execution of an infected file will cause all entries in the root directory to be changed to 'ZAPPED'. The virus is encrypted.

```
Pretoria           AC34 A5AA 4B75 F9C3 A11F 0150 A11D 01A3
```

PrintScreen - DR: Occasionally performs a Print Screen (PrtSc) operation.

```
Printscreen        FA33 C08E D0BC 00F0 1E16 1FA1 1304 2D02 ; Offset 023
```

Proud - CR: This 1302 byte virus is a member of a Bulgarian family of 4 viruses, which also includes 1226, Evil and Phoenix. As they all use the same encryption method, no search pattern is possible.(*VB* Dec 90)

Prudents - EN: Infective length is 1205 bytes and the virus will destroy the last 32 bytes of any infected file. Activates during the first four days of May of every year, turning every write operation into a verify operation, which results in the loss of data.

```
Prudents           0E07 BE4F 04B9 2300 5651 E87E 0359 5EE8 ; Offset 055
```

Rat - ER: This Bulgarian virus has been reported, but the sample which is available does not replicate.

```
Rat                FCB8 2B35 CD21 8CDD 0E1F 012E 6A0A BE10 ; Offset 0H
```

Russian Mirror - CR: This vicious virus from Russia trashes disks. Infective length is 482 bytes.

```
Russian Mirror     E89D FF80 FC4B 7403 E9C4 002E FE0E 6400
```

Saddam - CR: This virus extends the file length by 917 to 924 bytes. Displays the following string (which is stored encrypted)

```
HEY SADAM
LEAVE QUEIT BEFORE I COME
```

after 8 requests for INT 21H. Resides in the area of memory not labelled as used, so large programs will overwrite it.

```
Saddam             BB00 0153 5052 1E1E B800 008E D8A1 1304 ; Offset 010
```

Scott's Valley - CER: This virus is closely related to the Australian Slow virus, using an almost identical encryption method. It is somewhat longer, 2126 bytes.

```
Scott's Valley     E800 005E 8BDE 9090 81C6 3200 B912 082E
```

Shake - CR: A primitive 476 byte virus which reinfects already infected files. Infected programs sometimes reboot when executed. Occasionally, infected programs display the text "Shake well before use !" when executed.

```
Shake              B803 42CD 213D 3412 7503 EB48 90B4 4ABB
```

Slow - CER: This encrypted virus is a 1716 byte long mutation of the Jerusalem virus. It originates from Australia and its side-effects is reported to be a slow-down of the infected PCs. No other side-effects are known, as the virus is awaiting analysis.

```
Slow               E800 005E 8BDE 9090 81C6 1B00 B990 062E ; Offset 0
```

South African, Friday the 13th, Miami, Munich, Virus-B - CN: Infective length is 419 bytes, but some reports suggest mutations with an infective length between 415 and 544 bytes. Does not infect files with Read-Only flag set. Virus-B is a non-destructive mutation containing the South African 2 pattern. COMMAND.COM is not infected. Every file run on a Friday 13th will be deleted.

```
South African 1    1E8B ECC7 4610 0001 E800 0058 2DD7 00B1 ; Offset 158
South African 2    1E8B ECC7 4610 0001 E800 0058 2D63 00B1 ; Offset 158
```

Spanish Telecom - MCER: This encrypted virus contains a message by "Grupo Holokausto" demanding "lower telephone tariffs, more services". It proclaims to be an "Anti-CTNE" virus where CTNE is "Compania Telefonica Nacional Espana". A message in English states that the virus was programmed in Barcelona, Spain.(*VB* Jan 91)

```
Spanish_Head_1    8B1D B200 83FB 0074 18BF 5500 B2          ; Offset 034H
Spanish_Head_2    83ED 09BE 2001 03F5 FCB6                  ; Offset 024H
Spanish_Trojan    8A0E EC00 BE70 0003 F18A 4C02 8A74 03C3 ; Offset 0B3H in MBS
```

Subliminal - CR: This 1496 byte virus is probably an earlier version of the Dyslexia virus. When active, the virus will attempt to flash the message "LOVE, REMEMBER" on the screen for a fraction of a second, which is too short to be easily noticed.

```
Subliminal        AE26 3805 E0F9 8BD7 83C2 0306 1F2E C706 ; Offset 435
```

Sunday - CER: Variation of Jerusalem. Infective length is 1631 bytes (EXE) and 1636 (COM). Activates on Sunday and displays message "Today is SunDay! Why do you work so hard? All work and no play make you a dull boy.". There are unconfirmed reports of FAT damage on infected systems.

```
Sunday            FCB4 FFCD 2180 FCFF 7315 80FC 0472 10B4 ; Offset 095
```

Suomi - CN: A 1008 byte virus from Finland, which uses self-modifying encryption, like the Stealth virus. The virus seems to disinfect already infected files under certain conditions, but COMMAND.COM seems to remain permanently infected. No harmful side-effects have been reported, but the virus is awaiting disassembly. No search pattern is possible.

Suriv 1.01, April 1st COM - CR: A precursor to Jerusalem infecting only COM files with the virus positioned at the beginning of the file. Infective length is 897 bytes. If the date is 1st April, the virus will display "APRIL 1ST HA HA HA YOU HAVE A VIRUS" and the machine will lock. If the date is after 1st April 1988, the virus produces the message "YOU HAVE A VIRUS !!!" but the machine will not lock. The virus is memory resident and will not infect COMMAND.COM.(*VB* Aug 89)

```
Suriv 1.01        0E1F B42A CD21 81F9 C407 721B 81FA 0104 ; Offset 304, 897 bytes
```

Suriv 2.01, April 1st EXE - ER: A precursor to Jerusalem infectingEXE files with the virus positioned at the beginning of the file. Infective length is 1488 bytes. If the date is 1st April, the virus will display "APRIL 1ST HA HA HA YOU HAVE A VIRUS". If the year is 1980 (DOS default) or the day is Wednesday after 1st April 1988, the machine locksone hour after infection. (*VB* Aug 89)

```
Suriv 2.01        81F9 C407 7228 81FA 0104 7222 3C03 751E ; Offset 05E, 1488 bytes
```

Suriv 3.00, Israeli - CER: An earlier version of Jerusalem infecting COM and EXE files and displaying the side-effects 30 seconds after infection instead of 30 minutes. Infective length is 1813 bytes (COM) and 1808 bytes (EXE). Program delete does not work.
(*VB* Aug 89)

```
Suriv 3.00        03F7 2E8B 8D15 00CD 218C C805 1000 8ED0 ; Offset 0B0, 1813 COM, 1808 EXE
```

SVC - CER: A Russian, 1689 byte virus, containing the following message "(c) 1990 by SVC,Vers. 4.0". The virus attempts to avoid detection by the use of "stealth" methods, so any increase in file length is not visible while the virus is active in memory.

```
SVC               7416 80FC 1174 0E80 FC12 7409 9D2E FF2E ; Offset 142
```

Sverdlov - CER: A Russian, 1962 byte virus, using a simple XOR-encryption.

```
Sverdlov          2D00 03FE 2E30 0547 E2FA E800 005E 83EE ; Offset 019
```

Svir - EN: A simple 512 byte virus with no side-effects. Svir means "music" in Bulgarian.

```
Svir              33F6 4626 8B0C E302 EBF8 8BD6 83C2 04E8 ; Offset 049
```

Swap - DR: Does not infect until ten minutes after boot. One bad cluster on track 39, sectors 6 & 7 (head unspecified). Uses 2K of RAM. Infects floppy disks only. Does not store the original boot sector anywhere. Virus creates a display similar to Cascade, but is transmitted via boot sector.

```
Swap              31C0 CD13 B802 02B9 0627 BA00 01BB 0020 ; Offset ?
```

Sylvia - CN: The virus displays messages including "This program is infected by a HARMLESS Text-Virus V2.1", "You might get an ANTIVIRUS program....." when an infected program is executed, but if the above text is tampered with, the (encrypted) messages "FUCK YOU LAMER !!!!", "system halted....$" will be displayed. The victim is told to send a 'funny postcard' to a genuine address of a Dutch woman called Sylvia. When an infected program is run, the virus will look for five COM files on drive C and the current drive. COMMAND.COM, IBMBIO.COM and IBMDOS.COM are not infected. The virus adds 1301 bytes to the beginning of the infected files and 31 bytes at the end.

```
Sylvia            CD21 EBFE C3A1 7002 A378 0233 C0A3 9E02 ; Offset 229
```

Syslock - CEN: This encrypted virus attaches itself to the end of a COM or an EXE file. Infective length is 3551 bytes. It infects a program one in four times when executed. Will not infect if the environment contains SYSLOCK=@.

```
Syslock           8AE1 8AC1 3306 1400 3104 4646 E2F2 5E59 ; Offset 0, 3551 bytes
```

Taiwan - CN: The virus activates on the 8th day of every month and overwrites the FAT and the root directory of drives C and D. Two versions are known with different infection lengths: 708 and 743 bytes.

```
Taiwan          07E4 210C 02E6 21FB B980 0033 F6BB 8000 ; Offset 0A0
Taiwan (2)      07E4 210C 02E6 21FB B980 00BE 0000 BB80 ; Offset 065
```

Tenbyte, Valert - CER: This virus was by accident posted to the V-ALERT electronic mail list recently. Adds 1554 bytes to infected files. Activates on 1st September corrupting data written to disk.(*VB* April 90)

```
Tenbyte         1E0E 1F8D 36F7 04BF 0001 B920 00F3 A42E ; Offset 0
```

Terror - CER: This Bulgarian virus has not been analysed yet, as it failed to replicate under test conditions.

```
Terror          2E8C 1E41 0550 B859 ECCD 213B E875 3E0E ; Offset 046H
```

Tiny - CN: A mutation of the Kennedy virus only 163 bytes long. It has no side-effects other than replication.(*VB* Sept 90)

```
Tiny            408D 94AB 01B9 0200 CD21 B43E CD21 FFE5 ; Offset 088
```

Tiny Family - CR: This is a family of at least 10 Bulgarian viruses, which includes the shortest viruses now known. The viruses are not related to the Danish 'Tiny' virus, but just like it, they do nothing but replicate. The lengths of mutations range from 133 to 198 bytes.

```
Tiny Family (1) CD32 B43E CD32 071F 5F5A 595B 582E FF2E ; Offset variable
Tiny Family (2) 2687 85E0 FEAB E3F7 931E 07C3 3D00 4B75 ; Offset variable
```

TPworm - PN: A 'companion' virus written by the author of the Vacsina and Yankee Doodle viruses. The virus has been distributed in the form of 'C' source code. The infective length and hexadecimal patterns, hence, depend on the 'C' compiler used.

Traceback, Spanish - CER: This virus attaches itself to the end of a COM or an EXE file. Infective length is 3066 bytes. It becomes memory-resident when the first infected program is run and will infect any program run. If the date is 5th December or later, the virus will look for and infect one COM or EXE file either in the current directory or the first one found starting with the root directory. If the date is 28th December 1988 or later, the virus produces a display similar to Cascade one hour after infection. If nothing is typed, the screen restores itself after one minute. Display will repeat every hour. Spanish is an earlier version with a reported infective length of 2930 or 3031 bytes. (*VB* Sept 89)

```
Traceback       B419 CD21 89B4 5101 8184 5101 8408 8C8C ; Offset 104, 3066 bytes
Spanish         E829 06E8 E005 B419 CD21 8884 E300 E8CE ; Offset ?
```

Trackswap - DR: A small Bulgarian Master Boot Sector virus, which is awaiting analysis.

```
Trackswap       FBA1 1304 48A3 1304 B106 D3E0 8EC0 06BD ; Offset 00E
```

TUQ, RPVS - CN: A simple virus from West Germany without side-effects. Infective length is 453 bytes.

```
TUQ             5653 8CC8 8ED8 BE01 012E 8B04 0503 0157 ; Offset 05E
```

Turbo 448 - CR: A 448 byte Hungarian virus which will infect COM files when they are opened, for example by a virus scanner, but not when they are executed. The virus contains the text "Udv minden nagytudasunak! Turbo @"

```
Turbo 448       890E 0201 8CD8 8EC0 5958 BB00 01FF E3A1
```

Turbo Kukac - CR: A 512 byte virus, which resembles the Turbo 448 virus, but is somewhat longer, 512 bytes. COMMAND.COM will crash, if infected with this virus.

```
Turbo Kukac     FFE3 8CD8 488E D8A1 0300 2D41 00A3 0300
```

Typo, Typo COM, Fumble - CR: Infects all COM files in the subdirectory on odd days of every month. If typing fast, substitutes keys with the ones adjacent on the keyboard. Infective length is 867 bytes.(*VB* April 90)

```
Typo            5351 521E 0656 0E1F E800 005E 83EE 24FF ; Offset 01D, 867 bytes
```

V-1 - DCR: This virus was one of the first to infect both the boot sector and programs. It is 1253 bytes long and destructive: when activated, it overwrites the disk with garbage.

```
V-1             8EC0 26A1 1304 4848 503D 0001 7203 2D3E ; Offset 02B
```

V2P2 - CN; This virus, written by Mark Washburn of the United States, is closely related to the 1260 virus, but is more complicated. It will for example add a random number of "garbage" bytes to the programs it infects, to make identification more difficultAs with Washburn's other viruses, no search pattern is possible.

V2P6 - CN: This virus is written by the same author as 1260 and V2P2, but is longer and more complicated. It uses several different encryption methods, which makes it impossible to provide a signature string for the virus.

Vacsina - CER: Infective length 1206 to 1221 bytes (COM),1338 to 1353 bytes (EXE). After a successful infection of a COM file, a bell rings. Infects any file loaded via INT 21 function 4B (load and execute), i.e. COM, EXE, OVL and APP (GEM) files. Checks version number of itself (current is 5) and replaces with newer code. A member of the "Bulgarian 50" (see Yankee).(*VB* June 90)

```
Vacsina (1)     8CC8 8ED8 8EC0 8ED0 83C4 02B8 0000 502E ; Offset variable
Vacsina (2)     E800 005B 2E89 47FB B800 008E C026 A1C5 ; Offset variable
```

Vcomm - ER: This virus first increases the length of infected programs so that it becomes a multiple of 512 bytes. Then it adds 637 bytes to the end of the file. The resident part will intercept any disk write and change it into a disk read.

```
Vcomm           80FC 0375 04B4 02EB 0780 FC0B 7502 B40A ; Offset 261
```

VFSI - CN: A simple 437 byte Bulgarian virus.

```
VFSI            100E 1FB8 001A BA81 00CD 21BE 0001 FFE6 ; Offset 1A3
```

Victor - CEN: A 2442 byte virus from the USSR which is awaiting disassembly. The only known damaging effect is the corruption of the FAT.

```
Victor          8CC8 8BD8 B104 D3EE 03C6 50B8 D800 50CB ; Offset 0C8
```

Vienna, Austrian, Unesco, DOS62, Lisbon - CN: The virus infects the end of COM files. Infective length is 648 bytes. It looks through the current directory and the directories in the PATH for an uninfected COM file. One file in eight becomes overwritten. Seconds stamp of an infected file is set to 62. A number of mutations, shorter than the original, but functionally equivalent, have been reported in Bulgaria. (*VB* July 90)

```
Vienna (1)      8BF2 83C6 0A90 BF00 01B9 ; Offset 005, 648 bytes
Vienna (2)      FC8B F281 C60A 00BF 0001 B903 00F3 A48B ; Offset 004, 648 bytes
Vienna (3)      FC89 D683 C60A 90BF 0001 B903 00F3 A489 ; Offset 004
Vienna (4)      FC8B F283 C60A BF00 01B9 0300 F3A4 8BF2 ; Offset 004, 623 bytes
Vienna (5)      CD21 0E1F B41A BA80 00CD 2158 C3AC 3C3B ; Offset variable
Vienna (6)      8E1E 2C00 AC3C 3B74 093C 0074 03AA EBF4 ; Offset variable
```

Vienna-644 - CN: A 644 byte version of the Vienna virus, which does not infect programs every time it is run.

```
Vienna-644      BF00 01FC A5A5 A58B F252 B42C CD21 5A80
```

Violator - CN: This is an unsually long mutation of the Vienna virus. It is 1055 bytes long and it activates on 15th August. The virus is awaiting analysis.

```
Violator        BF00 01F3 A48B F2B4 30CD 213C 0075 03E9 ; Offset 00E
```

Virdem - CN: This virus was published in the R. Burger book *Computer Viruses - A High Tech Disease*. Originally intended as a demonstration virus, but now also found in the wild. Infective length is 1336 bytes. Two versions are known to exist with texts in English and German. (*VB* July 90)

```
Virdem          BE80 008D 3EBF 03B9 2000 F3A4 B800 0026 ; Offset 011
Virdem-1        BE80 008D 3ED7 03B9 2000 F3A4 B800 0026 ; Offset 011
Virdem-Gen      434B 7409 B44F CD21 72AC 4B75 F7B4 2FCD ; Offset 098
```

Virus-90 - CN: The author of this virus is Patrick A. Toulme. He uploaded the virus to a number of Bulletin Boards, stating that the source was available for $20. When an infected program is run it will display the message "Infected", infect a COM file in drive A and display the message "Done". Infective length is 857 bytes.

```
Virus-90        558B 2E01 0181 C503 0133 C033 DBB9 0900 ; Offset 01E
```

Virus-101 - CN: This virus was written by the same author as Virus-90. The virus is encrypted and self-modifying. An infected file has the seconds field set to 62. Will not infect if the first instruction in the file is not a 'JMP NEAR'. Infective length is 2560 bytes, but COMMAND.COM length does not change. Awaiting disassembly.

Virus-B - CN: 'Test virus' which was available as a restricted access file from the *Interpath Corporation* BBS in the USA. It is a mutation of the South African, with the destructive code of the original disabled. The identification pattern is the same as for the South African virus.

Voronezh - CER: A Russian, 1600 byte virus, which overwrites the first 1600 bytes of the host, and moves the original code to the end, where it is written in encrypted form.

```
Voronezh        3E89 078E C0BF 0001 BE00 015B 5301 DE0E
```

VP - CN: Contains a variable number (1 to 15) of NOPs at the beginning followed by 909 bytes of virus code. When an infected program is run, the virus may attempt to locate, infect and execute another program.

```
VP              0001 FCBF 0001 B910 00F2 A4B8 0001 FFE0 ; Offset variable
```

W13 - CN: A primitive group of viruses from Poland, based on the Vienna virus. They have no known side-effects and there are two versions, 534 and 507 bytes long. The version with 507 bytes has some bugs corrected.

```
W13     8BD7 2BF9 83C7 0205 0301 03C1 8905 B440    ; Offset variable
```

Westwood - CER: A 1824 byte mutation of the Jerusalem virus.

```
Westwood        4D0F CD21 8CC8 0510 008E D0BC 1007 50B8
```

Whale - CER: The infective length of this virus is 9216 bytes. The virus slows the system down by a factor of up to 50% and uses dynamic decryption of parts of its code. Much of the code is dedicated to disabling DEBUG to impede disassembly. The virus adopts one of thirty identities. Does not run on 8086-based computers.(*VB* Nov 90)

Wisconsin, Death to Pascal - CR: This virus adds 815 bytes to the beginning of infected programs, and 10 bytes to their end. Infected programs may display the message "Death to Pascal" and attempt to delete all .PAS files in the current directory.

```
Wisconsin          8B0E 0601 BE08 018A 0434 FF88 0446 E2F7 ; Offset 2F4
```

XA1 - CN: The XA1 virus overwrites the first 1539 bytes of infected COM files with a copy of itself and stores the original code at the end of the file. On 1st April the boot sector will be overwritten, causing the computer to 'hang' on the next boot. The virus will also activate on 21st December and stay active until the end of the year. It will then display a Christmas tree and the text:

```
Und er lebt doch noch: Der Tannenbaum!
Frohe Weihnachten
```

```
XA1 (1)            B02C 8846 FF8B 7E00 884E FE8A 4EFF 000D ; Offset 01E
XA1 (2)            0EE8 0000 FA8B EC58 32C0 8946 0281 4600 ; Offset 009
```

Yale, Alameda, Merritt - DR: This virus consists of a boot sector and infects floppies in drive A only. It becomes memory-resident and occupies 1K of RAM. The original boot sector is held in track 39 head 0 sector 8. The machine will hang if the virus is run on an 80286 or 80386 machine. If a warm boot is performed after the machine hangs, an uninfected disk will still become infected. It has not been assembled using MASM and contains code to format track 39 head 0, but this is not accessed. Survives a warm boot.

```
Yale               BB40 008E DBA1 1300 F7E3 2DE0 078E C00E ; Offset 009
```

Yankee - CER: This is a member of the "Bulgarian 50" group of viruses, which consists of some 50 related versions, all written by the same person. Vacsina viruses belong to the same group. All the viruses in the group will remove infections by older versions, and the size varies from 1200 to 3500 bytes. The Yankee viruses will play the tune "Yankee Doodle Dandy", either at 5:00 p.m. or when Ctrl-Alt-Del is pressed.

```
Yankee             0000 7402 B603 520E 5143 CFE8 0000 5B81 ; Offset variable
```

Zero Bug, Palette - CR: Infective length is 1536 bytes and the virus attaches itself to the beginning of COM files. The virus modifies the number of seconds to 62 (like Vienna). If the virus is active in memory and the DIR command is issued, the displayed length of infected files will be identical to that before the infection. When the virus activates, a "smiley" (IBM ASCII character 1) may appear on the screen, and "eat" all zeros found.

```
Zero Bug           81C9 1F00 CD21 B43E CD21 5A1F 59B4 43B0 ; Offset 100
```

REPORTED VIRUSES

382 - CN: Simple overwriting virus from Taiwan which overwrites part of the program.

1605 - CER: This virus is reported to be related to the Jerusalem virus, and to cause a slowdown of the system.

1702 - CR: A new mutation of the Cascade virus. Some doubt whether it exists.

Advent - CEN: Reported to be related to Macho and Syslock.

AirCop - DR: Virus may display the message "Red State, Germ Offensive. AIRCOP" or crash the system. Originated in Taiwan.

Arema - DR: Reported mutation of Den Zuk from Indonesia

Century A - CER: As Jerusalem-C, but activation date is 1st January 2000. Destroys FAT.

Century B - CER: As Jerusalem-C, but produces a wait during the execution of BACKUP.COM.

Chaos - DR: A new and changed mutation of Brain.

Freddy - CR?: Infects IBMBIO.COM

Hacker - DR: This virus from Indonesia is probably identical to Ohio.

Invader - DCER: Taiwanese virus reported to be related to the Plastique virus. It will play a melody 30 minutes after activation.

Jerusalem-A - CER: does not display black-hole in the screen.

Jerusalem-B - CER: EXE re-infection bug removed.

Jerusalem-C - CER: no slow-down effect.

Jerusalem-D - CER: destroys FAT in 1990.

Jerusalem-E - CER: destroys FAT in 1992.

Kitty - ?: This is not a virus, just a harmless modified boot sector, which will display the same message over and over if it is loaded.

```
Kitty    FABB C007 8ED3 BC7A 020E E800 005E 1F83    ; Offset 080
```

Mardi Bros - DR: A French virus which changes the Volume label to "Mardi Bros".

Mirror - ER: A 927 byte virus, which occasionally changes the video display, to produce a mirror image of what was there previously.

Missouri - D: some doubt whether it exists.

Nichols - D: some doubt whether it exists.

Number One - CN: An old, primitive virus, which was written three years ago and published in a book by Ralf Burger.

Novell - CER: A mutation of Jerusalem, reported to attack*Novell* networks. (*VB* Dec 90)

Ontario - CER: A 512 byte encrypted virus from Canada.

Park ESS: A new mutation of Jerusalem.

PC-club - DR: Reported in Indonesia. Said to display a message every 30 minutes.

PC-monster - DR: Closely related to Den Zuk.

Poem - ?

Polish 529 - CR; A 529 byte virus, which attaches itself to the beginning of infected programs. This virus may be identical to the 529 byte Anti-Pascal mutation, but a sample has not yet been made available.

Robert/Narvin - DR: An Indonesian virus which displays graphics on the screen.

Screen - CR: Infects all COM files in current directory, including any already infected, before becoming memory resident. Every few minutes it transposes two digits in any block of four on the screen.

Semlohe and Keongz - DR: An Indonesian virus based on Den Zuk, but producing sound effects.

Spyer - CER: A 1181 byte virus from Taiwan. Easily detected, as the computer will always hang after executing an infected program.

Supernova - DR: A harmful virus from Indonesia which will format the hard disk when the printer is used.

Taiwan 4 - CER: A 2576 byte virus, which appears to be related to the Plastique/AntiCAD viruses.

TCC - CER: A 4909 byte virus from France. Side-effects are unknown.

Terror - CER: This Bulgarian virus has not been analysed yet, as it failed to replicate under testing conditions.

Wolfman - CER: A 2064 byte virus from Taiwan.

TROJAN HORSES

AIDS Information Diskette: Widely distributed disk which is an extortion attempt. Installs multiple hidden directories and files, as well as AIDS.EXE in the main directory and REM$.EXE in a hidden subdirectory ($ is the non-printing character FF Hexadecimal). (*VB* Jan 90)

```
REM$.EXE          4D5A 0C01 1E01 0515 6005 0D03 FFFF 3D21 ; Offset 0
AIDS.EXE          4D5A 1200 5201 411B E006 780C FFFF 992F ; Offset 0
```

Twelve Tricks: A Trojan replacing the DOS Boot Sector with a dummy version. Damage includes corruption of the FAT and twelve effects which may be mistaken for hardware failure.

```
Twelve Tricks     BAB8 DBBE 6402 3194 4201 D1C2 4E79 F733 ; Offset 033
```

VIRUS ANALYSIS

Jim Bates

Spanish Telecom

Another virus attempting to make a political (?) point has recently come to hand from Spain. (The virus was identified at two separate academic sites - *Oxford University* and *City University*, London, UK, in December 1990, although no further reports of 'real world' infections have yet been received. Ed.) The virus has been called "Spanish Telecom" for reasons which will become apparent as this analysis progresses.

Multi-Partite Structure

This virus is a true multi-partite virus in that it functions both as a **parasitic virus** infecting COM files, and as a **boot sector** virus which infects the Master Boot Sector of the first fixed disk drive as well as the boot sector of **any** type of floppy disk. **The code contains a particularly vicious trigger routine which will overwrite all data on both the first and second fixed disk drives.** The trigger routine is invoked from the boot code section of the virus after the 400th infected boot cycle. The parasitic code is encrypted and contains plain text at the end of the code which reads:

```
Virus Anti - C.T.N.E. (c)1990 Grupo Holokausto.
Kampanya Anti-Telefonica. Menos tarifas y mas
servicios.Programmed in Barcelona (Spain). 23-8-90.
-666-
```

The final "666" may be a reference to the 666 (Number of the Beast) virus since certain techniques first noticed there have been used here! The phrase translates roughly as "Lower tariffs, more service." Another message which is separately encrypted is displayed during the overwriting activity of the trigger routine:

```
Campana Anti-TELEFONICA (Barcelona)
```

Analysis of this code is best undertaken by considering the parasitic and boot sections separately.

Parasitic Analysis

This is undoubtedly the most untidy code which I have examined. There are many repetitions and several bugs which will reveal the presence of the virus long before the trigger routine is invoked.

The virus code is attached at the end of COM files between 128 and 60999 bytes in length (inclusive). COMMAND.COM is specifically excluded from infection as is any file beginning with the letters "IBM" (the IBM system files). The initial four bytes of the host file are saved within the virus code and overwritten with an appropriate jump instruction to pass processing to the virus code.

The infective length of the parasitic code is 3,700 bytes (this includes the boot code). The virus code begins with an 85 byte section which contains "armoured" code to detect debugging software and several randomised instructions which are presumably intended to prevent the extraction of a reliable search string. There are two different versions of this 85 byte "header" routine, only one of which is actually positioned for use during the file infection process. There are, therefore, **two** distinct search strings for the parasitic code although each confirms the existence of the same virus.

Both "header" code routines perform the same functions: check for debug presence, locate the position of the virus code within the host segment and decrypt the remaining code.

Processing then checks to see whether the virus is memory-resident . This is done by collecting the byte at offset 1BCH of low memory and XORing it with 13H, the result is then checked against the next byte at offset 1BDH. If they are the same then the virus is resident and processing returns to the host program. The values of these two bytes are changed regularly by the virus during its intercept operations but by simply XORing them together, regardless of their values, the result will be 13H if the virus is resident in memory.

If the virus is not resident, the current INT 21H vector is collected and stored in memory via direct access to page zero of memory where the interrupt vectors are stored. The virus code is then installed in high memory and 3984 bytes are removed from system memory to accommodate it.

The next set of instructions collects a pseudo-random number from the system clock and uses it to index into a table of word addresses. The selected word is then inserted as the offset portion of the INT 21H vector in low memory, the segment portion being set to the virus' own segment in high memory. This random process of selection ensures that the actual offset stored in the interrupt table will vary from infection to infection. Each address, though different, points to a jump instruction which takes processing to a single INT 21H handler within the virus code. There are 14 entries in the address table although only 7 of them are used and this, together with other sections of the code, suggests that other techniques may have been tried (or are being prepared). Once the interrupt handler has been installed, a special call is made to it which completes the installation process. This call consists of putting 4B21H into AX and issuing an INT 21H request.

The special call is routed by the virus' handler to an installation routine which uses the single step INT 01H capability in the same way as the Flip virus (*VB*, Sept 90) to "strip" out any extraneous handlers from the targeted interrupt chain. Interrupts treated in this way are 13H, 21H and 40H and the stripped vectors are temporarily installed during file infection

and repaired when the process has completed. **Thus any TSR monitoring software which uses installed handlers will need to contain reliable self-testing routines to guard against this type of subversion.**

Interrupt Handling

The virus interrupt handler intercepts six different function requests within the DOS services interrupt: function 4B21H has already been mentioned and there is another special call using a value of 4B20H which does nothing. This gives rise to speculation that further developments may be planned. The SEEK function (42H) is intercepted when accompanied by subfunction 02 (to End of File). This checks to see whether the file has been infected and if so, modifies the pointer to subtract the length of the virus code before returning the End of File position. The two alternative sets of Find First and Find Next functions (11H - 12H and 4EH - 4FH) are similarly intercepted to return a modified file size on infected files.The main intercept however, is that applied to the Load and Execute function (4B00H). This is used to select and infect files with a COM extension (subject to the name and size exceptions mentioned earlier). Once a suitable file has been identified, the INT 13H and INT 40H vectors are temporarily replaced with their stripped equivalents and a simple handler for the critical error interrupt (24H) is installed.

The usual process of file infection is then invoked whereby the target file date, time and attributes are collected and stored, and the file is opened for Read/Write access (attributes are modified if necessary). The correct initial jump is calculated and the first four bytes of the target file copied and stored before being overwritten by a jump to the virus code. Certain sections of the virus code are then modified by the addition of random data values generated from a system clock reading.

The next stage involves using one of these data values as the new encryption key into one of the two 85 bytes decryption headers (chosen at random). The header is written (unencrypted) to the end of the host file. All the virus code is then encrypted and written to the end of the host file one byte at a time - each byte is collected, encrypted and written on an individual basis. This removes the need for a special buffer or a decrypt/recrypt cycle.

"The code contains a particularly vicious trigger routine which will overwrite all data on both the first and second fixed disk drives."

The final stage is to close the file and reset the date, time and attributes to their original settings. As a marker to indicate that the file is infected, the date setting is modified in a similar way to the 4K (or FRODO) virus by adding 100 to the year field. Modified interrupt vectors are reset to their previous values before processing returns to the calling routine.

During the installation of the handlers, a check is made to see whether the Master Boot Sector of the first hard drive is infected with the virus' boot code. If the disk is not infected then the boot section of the virus code is installed in Sector 1, Head 0, Track 0. The second sector of virus code is stored in sector 6 of the same track and the original boot sector is stored in sector 7. This will cause problems of access on some machines which use these sectors for other purposes.

Boot Sector Analysis

The boot section of this virus functions completely independently of the parasitic portion and both sections will almost certainly be in memory simultaneously. This may explain the almost obsessive concern with revectoring interrupts during the parasitic file infection. However, while the parasitic code contains all the virus routines, the boot section is limited to two sectors of self-contained code. **Thus a machine infected with only the boot code will not infect files, only other disks.**

The only items worthy of note in the boot code are the trigger routine, the floppy infection routine and the interrupt redirection. The interrupt redirection intercepts requests to INT 13H for both floppy and hard drives. A Read or Write request to either the first or second floppy drive will result in the disk being checked for infection and infected if possible. The routine is unusual in that it will only complete the check and infection if the motors of both the first two floppy drives are **not** running.

INT 13H requests to the first hard drive are intercepted and tested to see whether they are Read or Write. A Write request to the Master Boot Sector of the first hard drive is changed into a Verify call so that the sector will not be overwritten if the virus is resident. Read requests are tested to see which sector (on Head 0, Track 0) is wanted and re-routed accordingly. Requests for sector 1 are given sector 7 (where the original boot sector is stored) and requests for either sector 6 or 7 are given sector 5. **In a similar way to the Brain virus, Spanish Telecom, when resident, will attempt to prevent inspection of the true boot sector by ordinary utilities.**

Floppy Infection

If an uninfected floppy is accessed, the virus will attempt to infect it and the storage sectors used for the second sector of code will vary according to a table maintained within the virus code. **Remember that both first and second (A: and B:) drives are affected.**

Floppy disk infection indicating the head and sector location of the virus code on diskettes is shown in *Figure 1*.

Floppy Type	Virus Location	
	Head	Sector
160K - 5.25"	0	6
180K - 5.25"	0	8
320K - 5.25"	1	1
360K - 5.25"	1	2
720K - 5.25" or 3.5"	1	4
1.2M - 5.25"	1	0DH (decimal 13)
1.44M - 3.5"	1	0EH (decimal 14)

Figure 1. Spanish Telecom diskette infection locations

In *Figure 1* it will be seen that infected disks may become unreadable as virus code overwrites sections of the FAT or root directory. **To complete this information you should note that the virus code occupies sectors 1 and 6 of a hard disk, with copy of the original boot sector being stored in sector 7 (all on head 0, track 0).** (This is the first virus known to *VB* which will infect *all* diskettes regardless of density - the table above is a graphic reminder of the need to write-protect floppies, even those dedicated to pure data transfer. Ed.)

Trigger Routine

When a PC is booted from an infected hard disk, a counter within the boot code is incremented and tested to see whether it has passed 400 (190H). If it hasn't, the code is rewritten back to the boot sector and processing continues normally. However, when the counter does reach this number, processing immediately passes to the trigger routine. This is one of the nastiest, most destructive triggers I have seen; **it overwrites all sectors of both the first and (if there is one present) the second hard drive with random information from boot-time low memory**. The overwriting routine will be completed a number of times (for each drive) depending upon the number of heads on the drive. On each pass, the encrypted message reproduced on page 22 will be displayed.

Detection

It has been necessary to extract a different recognition string for each version of the parasitic code and these are as follows:

```
Header 1 - 8B1D B200 83FB 0074 18BF 5500 B2 ;
Offset 034H

Header 2 - 83ED 09BE 2001 03F5 FCB6 ; Offset 024H
```

It should be noted that the presence of **either** of these strings at the appropriate offset (into the virus code) is an indication of infection. Infective length of the parasite is 3700 bytes (appended on LOAD and EXECUTE).

Recognition of the boot virus code is simpler but note should be taken of the interrupt redirection discussed above. The code is not encrypted and the recognition string is as follows:

```
8A0E EC00 BE70 0003 F18A 4C02 8A74 03C3 ; Offset
0B3H
```

The Sabotage Mentality

The Spanish Telecom virus is demonstrative of a prevailing sabotage mentality. For example, preliminary analysis of the Plastique virus (its name is a reference to plastic explosive) has revealed a trigger routine which simulates an explosion through the PC's speaker and simultaneously overwrites all data on any hard disk found to be present. Equally insidious are the viruses which randomly scramble data stored on FATs such as NOMENKLATURA (*VB*, Dec 90) and those, like Disk Killer, which encrypt the hard disk.

The following annotations were added to an assembly (i.e. source code) listing of the Casper virus written by Mark Washburn of the United States. The final comments provide a chilling insight into the mind of the author. The code instructions are not reproduced here.

```
UTILITY.ASM - Manipulation Task For Casper The
Virus.
USAGE: Is automatically included in the assembly
of casper.asm
DETAILS: Date Activated Hard Disk Destroyer.
DATE: 1st April
DAMAGE: Formats Cylinder 0 of HD.

[the destruction routine]

db          "Hi! I'm Casper The Virus, And On
            April The 1st I'm"
db          "Gonna Fuck Up Your Hard Disk REAL
            BAD!"
db          "In Fact It Might Just Be Impossible
            To Recover!"
db          "How's That Grab Ya! <GRIN>"
```

Whether this destruction routine was included by Washburn, or by someone else is difficult to ascertain. Washburn is a prolific virus writer - 1260, V2P2 and V2P6 are among his other creations. At the beginning of the assembly listing (which is copyrighted) enquiries are directed to: *Mark Washburn, 4656 Polk Street NE, Columbia Heights, MN 55421, USA.*

PRODUCT REVIEW

Dr. Keith Jackson

Norton AntiVirus

The *Norton AntiVirus* program has recently been the subject of much publicity, having been launched, withdrawn, and then relaunched, in fairly quick succession (*VB*, Oct 90, p. 2). This review uses the latest version of *Norton AntiVirus* which has files dated as late as 12th December 1990. The master disk displays the serial number 1.0.0, so presumably this is the first *official* release of the *Norton AntiVirus*.

Documentation

The manual provided with *Norton AntiVirus* is clearly written as far as it goes, but is pitched at a fairly low level. This is fine for initial learning, but the style soon grows irksome. Most of the more interesting information is contained in an 855 line README file contained on the master disk. Given that the manual contains mainly bland descriptions of how to use *Norton AntiVirus*, the sheer size of the README file is daunting to say the least. The README file contains details of circumstances in which *Norton AntiVirus* is incompatible with other software, so beware.

Astonishingly, the only place that the *Norton AntiVirus* error messages are documented is in the README file. I find it inexplicable that anyone could write a user manual without documenting the error messages; reading an explanation of an error message is about the only reason I ever use a manual. Perhaps the time has already arrived for the documentation to be updated. Certainly the manual would benefit from some proof reading: I particularly like the phrase 'becuase it is disable by default'.

Installation

The *Norton AntiVirus* program is supplied on both 5.25 inch and 3.5 inch floppy disks. Both floppy disks are permanently write-protected; a sound practice which many other software houses should employ.

The install program provided with *Norton AntiVirus* is very easy to use. It offers clear straightforward choices. During the actual installation process, a horizontal bar graph shows how far installation has proceeded. However, on the version evaluated, when this bar graph indicated completion, many files had yet to be copied across to the hard disk, and installation still proceeded for some while. It appears that the installation program was written before various files were added to *Norton AntiVirus*. This looks incongruous, and mars an otherwise excellent installation program.

Operation

The two main components of *Norton AntiVirus* are **Virus Clinic** and **Virus Intercept**. Virus Clinic is a stand-alone program that can scan for the presence of viruses. Virus Intercept is a memory-resident program that detects the copying and/or execution of a virus infected file.

Virus Clinic

Virus Clinic offers a Windows-like interface, indeed PIF files are provided for use with Windows, but unfortunately the manual does not mention Windows in the table of contents or in the index. You need to search the README file for help on this subject. Choices can be made from drop-down menus either by using a mouse, or by using the Alt key and the first letter of the menu option. All very standard stuff, and given some familiarity with Windows style programs, very easy to use. One highly irritating feature is that after a menu has been displayed, and a choice made, the Esc key cancels an operation back to a clear screen, rather than just reverting back to the previous menu. There are also hidden (undocumented) shortcut keys; e.g. pressing the F10 key exits immediately to DOS whether or not this action was intended.

The manual insists on using the word 'definition' when referring to a pattern of bytes from a virus which are to be searched for within a file, as opposed to the almost universally used term 'signature'. I can think of no reason for muddying the waters by introducing another new term when there are already at least two (pattern, signature) in existence. A string of data defines nothing, so why use the word 'definition'?

The patterns searched for by Virus Clinic can be extended by the user, and purchase of *Norton AntiVirus* includes access to **Virus Newsline**, a hot-line telephone that can provide immediate access to new virus signatures. The version of *Norton AntiVirus* provided for test knew about 115 uniquely named viruses, with variants increasing this total to 142.

While scanning for viruses, Virus Clinic displays a horizontal bar to indicate how much progress has been made. This had only reached about 40 percent of its full range when the software realised that it had completed execution and immediately zoomed up to 100 percent. There seems to be little point in a progress indicator which is incorrect.

Speed and Detection Rate

Programs that detect viruses by scanning for known patterns are judgedby two criteria: how fast they can scan, and how well they can detect viruses.

I tested the scanning speed of *Norton AntiVirus* by searching the whole of my hard disk. It took 2 minutes 27 seconds to report that it had searched 1601 files, using its Basic mode of scanning which searches all files for known viruses.

For comparison purposes, version 4.5B66 of *SCAN* from *McAfee Associates* took 4 minutes 56 seconds to search the same disk, and version 2.13 of *SWEEP* from *Sophos* took 4 minutes and 30 seconds.

Advanced Scan

Norton AntiVirus can use an 'Advanced Scan' mode which creates a checksum file (a hidden file) associated with each executable file, the first time that a particular file is tested. However this suffers from the problem that a single small file is created for each and every checksum. The README file (not the manual) notes that although this file is at most 77 bytes long, depending on the version of DOS in use, it will occupy somewhere between 2 Kbytes and 8 Kbytes of disks space. On my hard disk, *Norton AntiVirus* searched 1601 files, so even using the smallest estimate of granularity, 'Advanced Scan' would consume 3.2 Mbytes of disk space. Using the figure of 8 Kbytes of actual disk space for each file, this becomes 12.8 Mbytes.

This is not very practical and I would venture to suggest that the Advanced Scan feature be re-submitted to the drawing board. Nobody will waste precious disk space on this scale, or clutter up their hard disk with hundreds of unnecessary files.

Worse (and acknowledged in the README file) is that each of these files is a hidden file, with the consequence that most programs that remove fragmentation from a hard disk (such as *Norton's Speed Disk*) will refuse to move such files; the hard disk becomes full of files that cannot be moved.

I tested the accuracy with which *Norton AntiVirus* could detect viruses by using the standard *VB* set of viruses (*see Technical Details below*), and it detected a virus on every single occasion except one variant of the Yankee virus. I encountered the usual differences in nomenclature, but disregarding this minor quibble, *Norton AntiVirus* correctly detected 100 out of the 101 virus test samples - a very impressive achievement.

Virus Intercept

Virus Intercept is a memory-resident program, which detects copying and/or execution of virus infected programs. This seemed to be as good at detecting viruses as the Virus Clinic program. Given that they use the same information about viruses, this is perhaps unsurprising.

However, it is inevitable that such monitoring introduces some detrimental effect on the speed at which files are copied.

To remove any effects introduced by files residing at differing places on a physical disk, I measured the overhead introduced by copying a file from one part of a RAM disk to another(a RAM disk is a portion of computer memory assigned as a disk drive).

The times to copy files of varying sizes are shown in the accompanying table. All figures are the average of at least three measurements.

File Size (bytes)	**Original Time** (seconds)	**Norton Anti-Virus** (seconds)
39515	0.67	1.96
53632	0.77	1.00
67769	0.91	1.39

I've reported these figures in some detail as the smallest of the three files tested (actually an executable copy of *Borland's Sidekick)*, shows the largest increase in copying time.

I can only speculate that the excellent speed of searching provided by *Norton AntiVirus* is achieved by using a quick search method as a first scan, and a more detailed search if the possibility of a byte pattern pertaining to a virus signature is detected. Inevitably some files will have to be searched in detail to ensure that viruses are not present. The above results show that Virus Intercept increases the time taken to copy a file by at least 25 percent, and possibly increases the copying time to 300 percent of the original. The *Norton AntiVirus* documentation should at least mention the overhead imposed by Virus Intercept.

As *Norton AntiVirus* is a memory-resident program, it is likely (probable?) that other memory-resident programs will not operate properly alongside Virus Intercept. The manual is silent about such problems, and the README file just mentions a list of programs with which Norton AntiVirus is known to be incompatible: 'Double-DOS, Referee, and other multitaskers/TSR managers'. The last category covers a range of possibilities. If you do encounter problems don't expect the documentation to provide helpful solutions. It won't.

Minor Points

I did not test the Repair facility provided with *Norton AntiVirus*, as I don't think that such an approach is a sensible way to deal with a virus infection. Secure deletion and reinstallation from an original source are safer remedies.

In common with nearly all other virus scanning programs, Norton AntiVirus has no knowledge of compressed programs of any kind. This includes all compressed archive files (ARC, LZH, PAK, ZIP or ZOO files). The README file, not the manual, states that 'Virus Intercept cannot detect infections in these files until they have been expanded. It will, however, prevent the viruses from being loaded into memory'. This is untrue for programs that have been compressed with a utility such as LZEXE (see *VB*, June 90, p.12) for later dynamic decompression. They will not be detected, will load normally, and can execute.

Conclusions

The Virus Clinic part of *Norton AntiVirus* scans for files very quickly and is extremely efficient at detecting viruses: a very worthwhile combination. Virus Intercept is just as efficient at detecting viruses, but introduces a permanent overhead on program loading and file copying.

The myriad faults in the documentation are mentioned at length in the above article. The package as a whole would benefit enormously by the inclusion of completely rewritten manual. In other respects, the *Norton AntiVirus* will prove a valuable addition to an anti-virus armoury - the speed and accuracy of the Virus Clinic component makes it a particularly valuable diagnostic tool.

Technical Details

Product: Norton AntiVirus

Vendor: Symantec (UK) Ltd., MKA House, 36 King Street, Maidenhead, Berkshire SL6 1EF, UK, Tel: (+44) 628 776343.

Developer: Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014, USA.

Availability: IBM PC, PS/2, or 100 percent compatible with either a 5.25 inch 360K floppy disk drive, a 3.5 inch 720K (or larger) floppy disk drive, or a hard disk. At least 384K of RAM is required, and MS-DOS v2.0 or above. Mouse usage is optional.

Version Evaluated: 1.0.0

Serial number: 100N00090

Price: £149 pounds sterling

Hardware: An Amstrad PPC640 with a V30 processor, and two 3.5 inch (720K) floppy disk drives, running under MS-DOS v3.30. Also a Toshiba 3100SX battery powered laptop with a 16Mhz 80386SX processor, one 3.5 inch (1.44M) floppy disk drive, and a 40Mbyte hard disk, running MS-DOS v4.01.

Viruses Test Set: This set of 49 unique viruses (according to the virus naming convention employed by *VB*), spread across 101 individual virus samples, is the standard *VB* test set. It comprises two boot viruses (Brain and Italian), and 99 parasitic viruses. There is more than one example of many of the viruses, ranging up to 10 different variants in the case of the Cascade and Vienna viruses. The actual viruses used for testing are listed below. Where more than one variant of a virus is available, the number of examples of each virus is shown in brackets. For a complete explanation of each virus, and the nomenclature used, please refer to the list of PC viruses published regularly in *VB*:

1260, 405 (2), 4K (2), AIDS, Alabama, Amstrad (2), Anarkia, Brain, Cascade (10), Dark Avenger (2), Datacrime (3), dBASE, December 24th, Devils Dance, Eddie (2), Fu Manchu (3), GhostBalls, Hallochen, Icelandic (2), Italian, Jerusalem (6), Kennedy, Lehigh, Macho-Soft, MIX1 (2), Number of the Beast, Oropax, Perfume, Prudents, PSQR, South African (2), Suriv (8), Sylvia, Syslock (2), Taiwan, Traceback (4), Typo, Vacsina, Valert, Vcomm, Vienna (10), Virdem, Virus-90, Virus-B (2), VP, W13 (2), XA-1, Yankee (5), Zero Bug,

VB POLICY

Product Evaluations

The virus test set used in product reviews is currently being expanded to encompass the newer generation of computer viruses. The new test set will include representative samples of: multi-partite infectors (which currently attack COM and EXE files and boot sectors); encrypting viruses (including those which employ a random decryption key);companion viruses (which shadow existing COM files by creating identical but infected EXE files); armoured viruses (which contain anti-disassembly code); and stealth viruses which appear 'invisible' in an infected operating environment. Details of the new test set will appear next month.

Search Patterns and Copyright

VB occasionally receives enquiries from individuals and software developers wishing to incorporate the hexadecimal search patterns which we publish in scanning or diagnostic software.

Some misunderstandings have arisen in the past about the copyright notice which appears at the foot of each page of the bulletin; *does this notification apply equally to hexadecimal search patterns?* The answer, of course, is an emphatic **NO** - **search patterns are not intellectual property or original material and are beyond copyright**. There have been incidents in the United States of software developers threatening lawsuits against other software developers on the basis that search patterns have been 'stolen'.

The *VB Table of Known IBM PC Viruses* is designed to be actively used; the patterns are supplied to help systems engineers with diagnosis but may also be used in the development of comprehensive scanning software. Use of these patterns is positively to be encouraged - commercial software and shareware which incorporates these patterns has performed well in tests.

However, a word of warning is warranted: **the published patterns should not be regarded as the basic intelligence with which to build scanning software - they serve more as supplementary information to enhance detection rates** One of the dangers associated with search patterns is that a hacker can render a virus undetectable by altering that portion of its code which has been published or made available.

Of greater significance, the latest viruses present no opportunity for a published pattern - detection being possible only by careful analysis of each program's structure. Moreover, the developers of disinfection software will, in nearly all cases, need access to the live virus before a suitable removal routine can be ascertained.

END-NOTES & NEWS

Correction

In the December 1990 edition of *VB* (p. 4), it was stated that a *CERT* advisory was posted on July 12th 1990 warning of a reported *Novell* virus. Ken van Wyk of the *Computer Emergency Response Team* has asked us to point out that this warning was not an official *CERT* Advisory but an independent posting from Dr. Jon David.

The *Virus Bulletin* Conference on Combating Computer Viruses, September 12-13th 1991, Hotel de France, St. Helier, Jersey. The full programme will be available in February. Speakers include Fridrik Skulason, Jim Bates, Vesselin Bontchev, David Ferbrache, Ross Greenberg, Jan Hruska, John Norstad, Yisrael Radai, Ken van Wyk and Gene Spafford. Specialist presentations on DOS, disassembly, forensics, anti-virus tools, recovery, Macs, DECNet/VMS, Unix, mainframes and networks, probable developments, malicious programming and corrupt work practices. Delegates are advised to book early due to demand. Information from Petra Duffield, *Virus Bulletin Conference*, UK. Tel 0235 531889.

The **ThunderByte PC Immunizer** is (according to the brochure) "capable of detecting and preventing ALL virus activity in EVERY PC, running under MS/PC-DOS". ThunderByte is an add on card which occupies 1 Kb of RAM and monitors unauthorised program activity. The developers *Novix International B.V.* of The Netherlands, also market **TB Scan**, a software virus-scanner. Tel *Novix International* (Holland) +31 8894 18957, BBS +31 85 212395.

Eliminator from *PC Security* Ltd follows VACCINE from *Sophos Ltd* as the second UK anti-virus software product to gain *CESG* certification. The product is certified to level UKL 1 following evaluation under *CESG's* CLEF scheme. (See *VB,* October 1990, p. 2.) Information from *PC Security*, UK. Tel 0628 890390.

Successive **seminars on Computer Viruses and Computer Security** will be presented Dr. Frederick B. Cohen, London, UK, 11th and 12th March 1990. Details from *IBC Technical Services,* UK. Tel 071 236 4080.

Cohen has also authored ***A Short Course on Computer Viruses***. The book costs US $48.00 including postage and packing. Available from *ASP Press,* PO Box 81270, Pittsburgh, PA 15217, USA.

A hire package to clean virus contaminated diskettes has been announced by *Softwarebuilders* and Dr. Alan Solomon. A special version of Solomon's Anti-Virus Toolkit runs on a portable PC linked to a Mountain Desktop Autoloader. *Softwarebuilders* claim that 300 diskettes per hour can be processed on an 80286 PC. The product can be hired for £225 per day. The device presumably derives from Dr. Solomon's earlier contraption 'D-MS-DOS'. Information from *S & S* (UK). Tel 0494 724201.

4th Annual Computer Virus & Security Conference 14-15th March 1991, New York, USA. *Computer Society of the IEEE*, USA. Tel 202 371 1013.

VIRUS BULLETIN

Subscription price for 1 year (12 issues) including delivery:

USA (first class airmail) US$350, Rest of the World (first class airmail) £195

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Abingdon, OX14 3YS, England

Tel (0235) 555139, International Tel (+44) 235 555139
Fax (0235) 559935, International Fax (+44) 235 559935

US subscriptions only:

June Jordan, Virus Bulletin, 590 Danbury Road, Ridgefield, CT 06877, USA
Tel 203 431 8720, Fax 203 431 8165